Tokeneer ID Station
System Test Specification

S.P1229.63.1
Issue: 1.1
Status: Definitive
19th August 2008

Originator

Janet Barnes (Project Manager)

Approver

David Cooper (Technical Authority)

Copies to:

NSA

Praxis High Integrity Systems
Project File

SPRE Inc

Contents

1 Introduction

1.1 Background

In order to demonstrate that developing highly secure systems to the level of rigour required by the higher assurance levels of the Common Criteria is possible, the NSA has asked Praxis High Integrity Systems to undertake a research project to develop part of an existing secure system (the Tokeneer System) in accordance with their high-integrity development process. This development work will then be used to show the security community that it is possible to develop secure systems rigorously in a cost effective manner.

1.2 Purpose

This document is the system test specification. This document specifies the system tests that are to be executed in order to demonstrate the correct behaviour of the system. Each test traces to the components of the Formal Design [1] that it demonstrates.

Analysis of the tracing then allows demonstration that all aspects of the Formal Design have been covered by these tests.

1.3 Structure

The next section describes the general test approach, it also provides usage instructions for the scripts that are utilised in the testing process.

Section 3 specifies the system tests themselves, for each test it gives the aims of the test, the initial state of the system before the test starts, the mechanism by which the test is run and the expected results.

2 Test Approach

All tests are scripted and should be run by starting TIS in the specified environment and executing a script file that triggers the SPRE test drivers into the required behaviour to perform the test.

In each case the state of the system at power-up will depend on the persistent data held within the Keystore, ConfigData and AuditLog.

Each test is run from a separate directory test/X. Where X is the name of the test. **tis** should be invoked from the directory test/TIS while the test stript , **testtis** should be invoked from the directory test/X.

In all cases the test script will issue instructions to the operator. So if **tis** has not been left running by the previous test then **testtis** should be started before **tis**.

It is intended that these tests should be run in the order supplied in this document. If a single test is run in isolation care should be taken to ensure that the initial state has been achieved for the test. This may involve running a few selected earlier tests as detailed in the initialisation table. In all cases the necessary **keystore** and **config.dat** files to set up the initial state are provided in the test/X/Temp directory. If the tests are not being run in order these two files should be moved to the System directory prior to starting TIS. Where possible the test script will set up the initial environment for the test, for example by ensuring that the door is initially closed and locked, in some cases one or other of the tokens needs to be present at the start of the test, where this is the case the test procedure details how to ensure that the appropriate token is in place prior to commencement of the test.

Many of the tests require specific card data to be loaded via one or other of the token readers. Where this is the case the source for the cards is provided within the test/X/Temp directory. This data can be processed to form a card and added to the SPRE database in a two-phase process using the **makecard** utility (see Section 2.2.2).

2.1 Script file format

The script file is a data file read by **testtis.** This makes modifications to the environment via peripherals and informs the tester of actions to be undertaken at each stage in the test.

The script file consists of commands presented on separate lines each command is either:

- a comment, any line starting with "- -" is considered a comment and will not be processed.
- **pause** N : an instruction to wait for N seconds before executing the next command.
- **print** text: and instruction to print the "text" on the console. This allows instructions to be presented to the tester.
- **hold**: an instruction to wait until the tester types <RETURN>. This allows the test script to be paused while the tester performs some action or waits for the system to perform a specific action.

- **displayOn** and **displayOff** these toggle the printing of the display data – display data is only printed when it changes and when **displayOn** is set. The default initial setting is **displayOff**.

- Call to a TDI (Test Driver Interface) as specified by SPRE Inc. These calls will be transmitted via TCP/IP to the SPRE test drivers.

2.2 Other useful test utilities

2.2.1 checkcard

The **checkcard** utility checks the data supplied in the file Temp/card.dat to ensure that it is consistent and can be validated by the current available **keystore**. The keystore used in this validation is retained in the file System/keystore. The utility outputs diagnostics demonstrating the aspects of the Card that are OK and aspects that are faulty and will fail checks.

2.2.2 makecard

The **makecard** utility has three options

- **make <cardid>** this operation takes the source from the file Temp/<cardid>.dat and converts it to a card. The resultant file is stored as Temp/card.dat. This is in a format suitable for checking with the checkcard facility. The format of the source file should be as follows:

  {'ATR': '**Number**',
  'cardInUse': '**BOOLEAN**'
  ***IDCERT
  {...<CertData dictionary>...}
  ***PRIVCERT
  {...<CertData dictionary>...}
  ***IACERT
  {...<CertData dictionary>...}
  ***AUTHCERT
  {...<CertData dictionary>...}
  ***END
  }

  The conversion strips all new lines and packs each of the certificate dictionaries appropriately. Each certificate is constructed using the initial *** tag to identify the certificate type and then the length fields are added to the certificate. Data prior to the first certificate is transferred to the card without any processing, as is data following the ***END tag.

  A <cardid> must start with the letter 'p' to conform to being a Praxis card.

- **add <cardid>** this operation submits the contents of Temp/card.dat to the SPRE card database with the card ID <cardid>.

A <cardid> must start with the letter ‘p’ to conform to being a Praxis card.

- **enrol <source>** this operation takes the source from the file Temp/<source>.dat and converts it to enrolment data. The source data for creating enrolment files takes the format:

  ```
  ***IDCERT
  {...<CertData dictionary>...}
  ***IDCERT
  {...<CertData dictionary>...}
  ***
  ```

  where each certificate is preceded by the ***IDCERT tag and the last certificate is followed by the *** tag. Each ID certificate is constructed from the provided CertData dictionary item and all new lines are stripped from this dictionary.

3 Test Cases

The following table summarises the test cases presented in this document:

Test name	Purpose
Enrolment 1	Start an un-enrolled TIS and attempt to enrol with bad enrolment data with too few certificates.
Enrolment 2	Start an un-enrolled TIS and attempt to enrol with bad enrolment data which has sufficient certificates but the third certificate is not signed correctly.
Enrolment 3	Start an un-enrolled TIS and perform a successful enrolment with 3 certificates.
UserEntry 1	Allow an administrator with role “Security Officer” to enter the enclave and acquire a valid Auth Certificate.
UpdateConfig 1	Logon the security officer as an administrator and update the configuration data and logout the security officer..
UserEntry 2	Allow an administrator with role “Guard” to acquire a valid Auth Certificate.
UserEntry 3	Allow an administrator with role “Guard” to enter the enclave without biometric checks.
Override 1	Logon the guard, attempt an operation that is not available to the guard and an operation that does not exist. Then perform the override door operation.
UserEntry 4	Attempt a user entry with a non-current ID certificate.
UserEntry 5	Attempt a user entry with a token with the I&A certificate signed by an unknown issuer.
UserEntry 6	Attempt a user entry with biometric data required. The user is slow providing a fingerprint so the entry fails.
UserEntry 7	Attempts a user entry with biometric data required. A non-matching fingerprint is supplied so the entry fails.
UserEntry 8	Allow a user to acquire a valid Auth Certificate. Guard logs out mid-operation.
UserEntry 9	Log on the guard and allow user to enter without biometric checks required.
AdminLogin 1	Attempt to logon a user with no admin privileges.
AdminLogin 2	Attempt to logon an Audit Manager with no Auth Certificate.
UserEntry 10	An administrator with role “Audit Manager” attempts entry but tears their token before finger validation.

Test name	Purpose
UserEntry 11	An administrator with role “Audit Manager” attempts entry but tears their token during finger validation.
UserEntry 12	Allow an administrator with role “Audit Manager” to acquire an Auth Certificate and enter the enclave.
UpdateConfig 2	Logon a security officer and attempt to change the configuration data using invalid configuration data.
UpdateConfig 3	Update the configuration data to an all hours configuration with very short validity period.
AdminLogout 1	Allow an administrator with role “Guard” to enter the enclave (and acquire an Auth Certificate) then logon as an administrator. Leave the guard logged on until their Auth Certificate expires when they will be automatically logged off.
AdminLogin 3	Guard attempts to logon as an administrator after their token has expired.
UpdateConfig 4	Security officer logs on and starts an Update config data operation but removes the token before the operation is complete.
UpdateConfig 5	Security officer successfully updates the configuration data to a working hours policy.
Shutdown 1	A user enters the enclave, before the door is closed the security officer performs a shutdown operation. Security officer removes token before the shutdown operation is complete – this does not affect the operation.
ArchiveLog 1	An audit manager logs on and starts an archive activity. The floppy is removed too soon causing the archive to fail.
ArchiveLog 2	An audit manager starts an archive activity, which fails since the data on the floppy does not match the archived data.
ArchiveLog 3	An audit manager successfully performs an archive operation and logs out.
UserEntry 13	A user provides a valid token for entry but there is a failure when signing the Auth Certificate so the certificate is not written. The user still gains entry to the enclave.
UserEntry 14	A security officer logs on and changes the configuration data so that working hours are only late at night. A user then attempts entry with a valid token but the signing fails and the Auth Certificate is not written. The user is denied entry since the current time is not within the entry times. The security officer then logs off.
Shutdown 2	A security officer logs on and successfully performs a shutdown
Truncate 1	The system exceeds its log capacity causing truncation of the log.

3.1 Enrolment 1

ST.Enrolment.1.FailedBadData1

FD.TIS.TISStartup
FD.Enclave.TISEnrolOp
FD.Enclave.RequestEnrolment
FD.Enclave.ReadEnrolmentFloppy
FD.Enclave.ValidateEnrolmentDataFail
FD.Enclave.WaitingFloppyRemoval
FD.Enclave.FailedEnrolFloppyRemoved
FD.AuditLog.LogChange

CVS repository: test\Enrol1.

3.1.1 Purpose

Start an un-enrolled TIS and attempt enrolment with faulty enrolment data. The faulty enrolment data consists of insufficient certificates.

3.1.2 Initial State

	Entity	State
TIS persistent state	Keystore	Absent
	AuditLog	Empty
	ConfigData	Absent

3.1.3 Test Procedure

Run test script and perform required actions.

3.1.4 Expected Results

3.1.4.1 Audited Events

Id	Severity	User	Description
StartUnenrolledTIS	1	No User	-
ScreenChanged	1	No User	PLEASE INSERT ENROLMENT DATA FLOPPY
ScreenChanged	1	No User	VALIDATING ENROLMENT DATA PLEASE WAIT
ScreenChanged	1	No User	INVALID ENROLMENT DATA
EnrolmentFailed	2	No User	Enrolment failed at certificate 2 - Certificate could not be verified
ScreenChanged	1	No User	PLEASE INSERT ENROLMENT DATA FLOPPY

3.1.4.2 Keystore

Empty.

3.1.4.3 Config data

Unchanged.

3.1.4.4 Visual

Screen Entity	**Status**
Door Alarm	OK throughout test
Audit Alarm	OK throughout test
Configuration Data	Never displayed
System Stats	Never displayed
Messages	Values as detailed in audit log ScreenChanged entries.

3.2 Enrolment 2

ST.Enrolment.2.FailedBadData2

FD.TIS.TISStartup
FD.Enclave.TISEnrolOp
FD.Enclave.ReadEnrolmentFloppy
FD.Enclave.ValidateEnrolmentDataFail
FD.Enclave.WaitingFloppyRemoval
FD.Enclave.FailedEnrolFloppyRemoved
FD.Enclave.RequestEnrolment
FD.AuditLog.LogChange

CVS repository: test\Enrol2.

3.2.1 Purpose

Start an un-enrolled TIS and attempt enrolment with faulty enrolment data. The faulty enrolment data has 3 certificates but the third certificate is corrupt.

Forces door before successful enrolment to ensure that TIS reports a security breach.

Closes door before terminating test.

3.2.2 Initial State

	Entity	State
TIS persistent state	Keystore	Absent
	AuditLog	Empty
	ConfigData	Absent

3.2.3 Test Procedure

Run test script and perform the requested actions.

3.2.4 Expected Results

3.2.4.1 Audited Events

Id	Severity	User	Description
StartUnenrolledTIS	1	No User	-
ScreenChanged	1	No User	VALIDATING ENROLMENT DATA PLEASE WAIT
ScreenChanged	1	No User	INVALID ENROLMENT DATA
EnrolmentFailed	2	No User	Enrolment failed at certificate 3 - Certificate could not be verified
ScreenChanged	1	No User	PLEASE INSERT ENROLMENT DATA FLOPPY
DoorOpened	1	No User	
AlarmRaised	3	No User	
DoorClosed	1	No User	
AlarmSilenced	1	No User	

3.2.4.2 Keystore

Empty.

3.2.4.3 Config data

Unchanged.

3.2.4.4 Visual

Screen Entity	**Status**
Door Alarm	Initially OK. Then FAIL following forcing the door. Finally OK.
Audit Alarm	OK throughout test
Configuration Data	never displayed
System Stats	never displayed
Messages	values as detailed in audit log ScreenChanged entries.

3.3 Enrolment 3

ST.Enrolment.3.Success

FD.TIS.TISStartup
FD.Enclave.TISEnrolOp
FD.Enclave.ReadEnrolmentFloppy
FD.Enclave.ValidateEnrolmentDataOK
FD.AuditLog.LogChange

CVS repository: test\Enrol3.

3.3.1 Purpose

Start an un-enrolled TIS and perform enrolment with good enrolment data.

3.3.2 Initial State

	Entity	State
TIS persistent state	Keystore	Absent
	AuditLog	Empty
	ConfigData	Absent

3.3.3 Test Procedure

Run test script and perform the requested actions.

3.3.4 Expected Results

3.3.4.1 Audited Events

Id	Severity	User	Description
StartUnenrolledTIS	1	No User	-
ScreenChanged	1	No User	VALIDATING ENROLMENT DATA PLEASE WAIT
ScreenChanged	1	No User	WELCOME TO TIS
DisplayChanged	1	No User	WELCOME TO TIS / ENTER TOKEN
EnrolmentComplete	1	No User	

3.3.4.2 Keystore

keystore file should contain 4 entries, one private key and 3 public keys.

Owner.ID	Owner.Text	KeyID	KeyLength	IsPublic
4294967295	TheTISIssuer	1	128	Y
1	ThisTISName	2	128	Y
1	ThisTISName	2	128	N
32767	AnAAMachine	3	64	Y

3.3.4.3 Config data

Unchanged.

3.3.4.4 Visual

Screen Entity	**Status**
Door Alarm	OK throughout test
Audit Alarm	OK throughout test
Configuration Data	never displayed
System Stats	never displayed
Messages	values as detailed in audit log ScreenChanged entries.

3.4 UserEntry 1

ST.UserEntry.1.NoAuthSuccess

FD.UserEntry.TISReadUserToken
FD.UserEntry.BioCheckRequired
FD.UserEntry.ReadFingerOK
FD.UserEntry.ValidateFingerOK
FD.UserEntry.ConstructAuthCert
FD.UserEntry.WriteUserTokenOK
FD.UserEntry.EntryOK
FD.UserEntry.UnlockDoorOK
FD.AuditLog.LogChange

CVS repository: test\UserEntry1.

3.4.1 Purpose

Allow an administrator with role “Security Officer” to enter the enclave and acquire a valid Auth Certificate.

The administrator enters the enclave successfully and obtains a card with valid auth certificate.

This test is a prelude to being able to update the configuration data.

3.4.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	-
	ConfigData	Absent
Initial Environment	Door	closed
	Latch	locked
	UserToken	absent
	AdminToken	absent
	Finger	absent
	Floppy	absent

3.4.3 Test Procedure

Run test script and perform the requested actions.

This test requires the use of a Security officer's card with no Auth Cert present.

3.4.4 Expected Results

3.4.4.1 Audited Events

Id	Severity	User	Description
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
ScreenChanged	1	No User	SYSTEM BUSY PLEASE WAIT
UserTokenPresent	1	Issuer: 4294967295 SerialNo: 100000001	
AuthCertInvalid	1	Issuer: 4294967295 SerialNo: 100000001	
DisplayChanged	1	No User	AUTHENTICATING USER / INSERT FINGER
FingerDetected	1	Issuer: 4294967295 SerialNo: 100000001	
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
FingerMatched	1	Issuer: 4294967295 SerialNo: 100000001	
AuthCertWritten	1	Issuer: 4294967295 SerialNo: 100000001	
EntryPermitted	1	Issuer: 4294967295 SerialNo: 100000001	
DisplayChanged	1	No User	/ REMOVE TOKEN AND ENTER
LatchUnlocked	1	No User	
DisplayChanged	1	No User	/ ENTER ENCLAVE
ScreenChanged	1	No User	WELCOME TO TIS
DoorOpened	1	No User	
DoorClosed	1	No User	
LatchLocked	1	No User	
DisplayChanged	1	No User	WELCOME TO TIS / ENTER TOKEN

3.4.4.2 Keystore

keystore is unchanged.

3.4.4.3 Config data

Unchanged.

3.4.4.4 Visual

Screen Entity	Status
Door Alarm	OK throughout test
Audit Alarm	OK throughout test
Configuration Data	Never displayed.
System Stats	Never displayed.
Messages	Values as detailed in audit log ScreenChanged entries.

3.5 UpdateConfig 1

ST.UpdateConfig.1.Success

FD.Enclave.TISAdminLogin
FD.Enclave.GetPresentAdminToken
FD.Enclave.ValidateAdminTokenOK
FD.Enclave.TISStartAdminOp
FD.Enclave.ValidateOpRequestOK
FD.Enclave.TISUpdateConfigDataOp
FD.Enclave.StartUpdateConfigDataOK
FD.Enclave.FinishUpdateConfigDataOK
FD.Enclave.TISAdminLogout
FD.Enclave.AdminLogout
FD.AuditLog.LogChange

CVS repository: test\UpdateConfig1.

3.5.1 Purpose

Update the configuration data.

To do this we need an administrator with role “Security Officer” to enter the enclave and acquire a valid Auth Certificate(done in test UserEntry1). This administrator must then logon and perform update configuration data operation with good configuration data.

Finally the Admin token is removed to log out the administrator.

3.5.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	Empty
	ConfigData	Absent

3.5.3 Test Procedure

Run test script and perform the requested actions.

This test requires the use of security officer’s card with an Auth Certificate present. Such a card can be obtained by running test UserEntry1.

This test also requires the use of config data supplied on a floppy.

3.5.4 Expected Results

3.5.4.1 Audited Events

Id	Severity	User	Description
AdminTokenPresent	1	Issuer: 4294967295 SerialNo: 100000001	
AdminTokenValid	1	Issuer: 4294967295 SerialNo: 100000001	
ScreenChanged	1	No User	ENTER REQUIRED OPERATION
ScreenChanged	1	No User	PERFORMING OPERATION PLEASE WAIT
OperationStart	1	Issuer: 4294967295 SerialNo: 100000001	UPDATE CONFIG
ScreenChanged	1	No User	INSERT CONFIGURATION DATA FLOPPY
ScreenChanged	1	No User	PERFORMING OPERATION PLEASE WAIT
UpdatedConfigData	1	Issuer: 4294967295 SerialNo: 100000001	20; 30; 15; 20; CONFIDENTIAL; 07:30; 17:30; 02:00; WORKINGHOURS; RESTRICTED; 1000; 260; 1000
ScreenChanged	1	No User	ENTER REQUIRED OPERATION
AdminTokenRemoved	1	Issuer: 4294967295 SerialNo: 100000001	
ScreenChanged	1	No User	WELCOME TO TIS

3.5.4.2 Keystore

keystore is unchanged.

3.5.4.3 Config data

Changed, the file System/config.dat should have the same contents as the file provided on floppy.

3.5.4.4 Visual

Screen Entity	Status
Door Alarm	OK throughout test
Audit Alarm	OK throughout test
Configuration Data	Displayed while SecurityOfficer logged on and changes to match supplied config file.
System Stats	Displayed while Admin logged on.
Messages	values as detailed in audit log ScreenChanged entries.

3.6 UserEntry 2

ST.UserEntry.2.NoAuthSuccess

FD.UserEntry.TISReadUserToken
FD.UserEntry.BioCheckRequired
FD.UserEntry.ReadFingerOK
FD.UserEntry.ValidateFingerOK
FD.UserEntry.ConstructAuthCert
FD.UserEntry.WriteUserTokenOK
FD.UserEntry.EntryOK
FD.UserEntry.UnlockDoorOK
FD.AuditLog.LogChange

CVS repository: test\UserEntry2.

3.6.1 Purpose

Allow an administrator with role “Guard” to acquire a valid Auth Certificate.

The guard obtains a card with valid auth certificate. The guard does not enter the enclave at this point.

This test is a prelude to being able to override door lock.

3.6.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	-
	ConfigData	config data created by UpdateConfig1 test

3.6.3 Test Procedure

Run test script and perform the requested actions.

This test requires the use of a Guard’s card with no Auth Cert present. The card information is held in **p02.dat**.

The guard does not go through the door at this point.

3.6.4 Expected Results

3.6.4.1 Audited Events

Id	Severity	User	Description
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
ScreenChanged	1	No User	SYSTEM BUSY PLEASE WAIT
UserTokenPresent	1	Issuer: 4294967295 SerialNo: 100000002	
AuthCertInvalid	1	Issuer: 4294967295 SerialNo: 100000002	
DisplayChanged	1	No User	AUTHENTICATING USER / INSERT FINGER
FingerDetected	1	Issuer: 4294967295 SerialNo: 100000002	
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
FingerMatched	1	Issuer: 4294967295 SerialNo: 100000002	
AuthCertWritten	1	Issuer: 4294967295 SerialNo: 100000002	
EntryPermitted	1	Issuer: 4294967295 SerialNo: 100000002	
DisplayChanged	1	No User	/ REMOVE TOKEN AND ENTER
LatchUnlocked	1	No User	
DisplayChanged	1	No User	/ ENTER ENCLAVE
ScreenChanged	1	No User	WELCOME TO TIS
LatchLocked	1	No User	
DisplayChanged	1	No User	WELCOME TO TIS / ENTER TOKEN

3.6.4.2 Keystore

keystore is unchanged.

3.6.4.3 Config data

Unchanged.

3.6.4.4 Visual

Screen Entity	Status
Door Alarm	OK until user holds door open too long. Then raised and cleared a few seconds later when door is closed.
Audit Alarm	OK throughout test
Configuration Data	Never displayed.
System Stats	Never displayed.
Messages	Values as detailed in audit log ScreenChanged entries.

3.7 UserEntry 3

ST.UserEntry.3.WithAuthSuccess
FD.UserEntry.TISReadUserToken *FD.UserEntry.BioCheckNotRequired* *FD.UserEntry.EntryOK* *FD.UserEntry.UnlockDoorOK* *FD.AuditLog.LogChange*
CVS repository: test\UserEntry3.

3.7.1 Purpose

Allow an administrator with role “Guard” to enter the enclave without biometric checks.

The door is held open too long during entry causing an alarm to be momentarily raised.

3.7.2 Initial State

	Entity	**State**
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	-
	ConfigData	config data created by UpdateConfig1 test

3.7.3 Test Procedure

Run test script and perform the requested actions.

This test requires the use of a Guard’s card with an Auth Cert present. Such a card can be obtained by running test UserEntry2.

3.7.4 Expected Results

3.7.4.1 Audited Events

Id	Severity	User	Description
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
ScreenChanged	1	No User	SYSTEM BUSY PLEASE WAIT
UserTokenPresent	1	Issuer: 4294967295 SerialNo: 100000002	
AuthCertValid	1	Issuer: 4294967295 SerialNo: 100000002	
EntryPermitted	1	Issuer: 4294967295 SerialNo: 100000002	
DisplayChanged	1	No User	/ REMOVE TOKEN AND ENTER
LatchUnlocked	1	No User	
DisplayChanged	1	No User	/ ENTER ENCLAVE
ScreenChanged	1	No User	WELCOME TO TIS
DoorOpened	1	No User	
LatchLocked	1	No User	
DisplayChanged	1	No User	WELCOME TO TIS / ENTER TOKEN
AlarmRaised	3	No User	
DoorClosed	1	No User	
AlarmSilenced	1	No User	

3.7.4.2 Keystore

keystore is unchanged.

3.7.4.3 Config data

Unchanged.

3.7.4.4 Visual

Screen Entity	Status
Door Alarm	OK until user holds door open too long. Then raised and cleared a few seconds later when door is closed.
Audit Alarm	OK throughout test
Configuration Data	Never displayed.
System Stats	Never displayed.
Messages	Values as detailed in audit log ScreenChanged entries.

3.8 Override 1

ST.Override.1.Success

FD.Enclave.TISAdminLogin
FD.Enclave.GetPresentAdminToken
FD.Enclave.ValidateAdminTokenOK
FD.Enclave.TISStartAdminOp
FD.Enclave.ValidateOpRequestFail
FD.Enclave.ValidateOpRequestOK
FD.Enclave.TISUnlockDoorOp
FD.Enclave.OverrideDoorLockOK
FD.AuditLog.LogChange

CVS repository: test\Override1.

3.8.1 Purpose

Allow an administrator with role “Guard” to log on, attempt to perform an operation that is not available to a guard, and an operation that does not exist. Then performs the override door lock operation successfully.

This test demonstrates Overriding the door lock and validation of operation requests.

3.8.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	-
	ConfigData	config data created by UpdateConfig1 test

3.8.3 Test Procedure

Run test script and perform the requested actions.

This test requires the use of a Guard’s card with an Auth Cert present. Such a card can be obtained by running test UserEntry2.

3.8.4 Expected Results

3.8.4.1 Audited Events

Id	Severity	User	Description
AdminTokenPresent	1	Issuer: 4294967295 SerialNo: 100000002	
AdminTokenValid	1	Issuer: 4294967295 SerialNo: 100000002	
ScreenChanged	1	No User	ENTER REQUIRED OPERATION
ScreenChanged	1	No User	INVALID REQUEST- PLEASE ENTER NEW OPERATION
InvalidOpRequest	1	Issuer: 4294967295 SerialNo: 100000001	UPDATE CONFIG
InvalidOpRequest	1	Issuer: 4294967295 SerialNo: 100000001	GARBAGE
ScreenChanged	1	No User	PERFORMING OPERATION PLEASE WAIT
OperationStart	1	Issuer: 4294967295 SerialNo: 100000001	OVERRIDE
OverrideLock	1	Issuer: 4294967295 SerialNo: 100000001	
ScreenChanged	1	No User	ENTER REQUIRED OPERATION
DisplayChanged	1	No User	/ ENTER ENCLAVE
LatchUnlocked	1	No User	
DoorOpened	1	No User	
DoorClosed	1	No User	
LatchLocked	1	No User	
DisplayChanged	1	No User	WELCOME TO TIS / ENTER TOKEN

3.8.4.2 Keystore

keystore is unchanged.

3.8.4.3 Config data

Unchanged.

3.8.4.4 Visual

Screen Entity	Status
Door Alarm	OK throughout test
Audit Alarm	OK throughout test
Configuration Data	Never displayed.
System Stats	Displayed once guard is logged on.
Messages	Values as detailed in audit log ScreenChanged entries.

3.9 UserEntry 4

ST.UserEntry.4.NoAuthFail

FD.UserEntry.TISReadUserToken
FD.UserEntry.ValidateUserTokenFail
FD.UserEntry.FailedAccessTokenRemoved
FD.Stats.Update
FD.AuditLog.LogChange

CVS repository: test\UserEntry4.

3.9.1 Purpose

A user attempts entry with a non-current ID certificate on their token. Entry should be denied and no Auth cert written.

Observe change in Stats, with a failed entry being logged.

3.9.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	-
	ConfigData	config data created by UpdateConfig1 test
	AdminToken	guard present (p02)

3.9.3 Test Procedure

Run test script and perform the requested actions.

This test requires a guard to be present, this can be achieved by running test Override1.

This test requires the a card with a non-current ID Cert present. The card information is held in **p03.dat**.

3.9.4 Expected Results

3.9.4.1 Audited Events

Id	Severity	User	Description
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
ScreenChanged	1	No User	SYSTEM BUSY PLEASE WAIT
UserTokenPresent	1	Issuer: 4294967295 SerialNo: 100000003	
UserTokenInvalid	2	Issuer: 4294967295 SerialNo: 100000003	ID Certificate Not Current
DisplayChanged	1	No User	ENTRY DENIED /REMOVE TOKEN
ScreenChanged	1	No User	ENTER REQUIRED OPERATION
userTokenRemoved	1	Issuer: 4294967295 SerialNo: 100000003	
DisplayChanged	1	No User	WELCOME TO TIS / ENTER TOKEN

3.9.4.2 Keystore

keystore is unchanged.

3.9.4.3 Config data

Unchanged.

3.9.4.4 Visual

Screen Entity	**Status**
Door Alarm	OK throughout test
Audit Alarm	OK throughout test
Configuration Data	Never displayed.
System Stats	Displayed and number of failed entries should increment.
Messages	Values as detailed in audit log ScreenChanged entries.

3.10 UserEntry 5

ST.UserEntry.5.NoAuthFail

FD.UserEntry.TISReadUserToken
FD.UserEntry.ValidateUserTokenFail
FD.UserEntry.FailedAccessTokenRemoved
FD.Stats.Update
FD.Enclave.TISStartAdminOp
FD.Enclave.OverrideDoorLockOK
FD.Enclave.TISUnlockDoorOp
FD.AuditLog.LogChange

CVS repository: test\UserEntry5.

3.10.1 Purpose

A user with an I&A certificate signed by an unknown issuer on their token attempts entry while the guard is logged on. Entry should be denied and no Auth cert written.

Additionally the guard overrides the door lock before the failed token has been removed. This is done to check that the correct message appears on the display following the door being relocked.

Observe change in Stats, with a failed entry being logged.

3.10.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	-
	ConfigData	config data created by UpdateConfig1 test
	AdminToken	guard present (p02)

3.10.3 Test Procedure

Run test script and perform the requested actions.

This test requires a guard to be present, this can be achieved by running test Override1.

This test requires a card with a no Auth Cert and an invalid I&A Cert present. The card information is held in **p04.dat**.

3.10.4 Expected Results

3.10.4.1 Audited Events

Id	Severity	User	Description
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
ScreenChanged	1	No User	SYSTEM BUSY PLEASE WAIT
UserTokenPresent	1	Issuer: 4294967295 SerialNo: 100000004	
UserTokenInvalid	2	Issuer: 4294967295 SerialNo: 100000004	I&A Certificate Not Verifiable
DisplayChanged	1	No User	ENTRY DENIED /REMOVE TOKEN
ScreenChanged	1	No User	ENTER REQUIRED OPERATION
ScreenChanged	1	No User	PERFORMING OPERATION PLEASE WAIT
OperationStart	1	Issuer: 4294967295 SerialNo: 100000002	OVERRIDE
OverrideLock	1	Issuer: 4294967295 SerialNo: 100000002	
ScreenChanged	1	No User	ENTER REQUIRED OPERATION
DisplayChanged	1	No User	/ ENTER ENCLAVE
LatchUnlocked	1	No User	
LatchLocked	1	No User	
DisplayChanged	1	No User	ENTRY DENIED /REMOVE TOKEN
userTokenRemoved	1	Issuer: 4294967295 SerialNo: 100000004	
DisplayChanged	1	No User	WELCOME TO TIS / ENTER TOKEN

3.10.4.2 Keystore

keystore is unchanged.

3.10.4.3 Config data

Unchanged.

3.10.4.4 Visual

Screen Entity	Status
Door Alarm	OK throughout test
Audit Alarm	OK throughout test
Configuration Data	Never displayed.
System Stats	Always displayed, failed entries should increment.
Messages	Values as detailed in audit log ScreenChanged entries.

3.11 UserEntry 6

ST.UserEntry.6.NoAuthFail

FD.UserEntry.TISReadUserToken
FD.UserEntry.BioCheckRequired
FD.UserEntry.NoFinger
FD.UserEntry.FingerTimeout
FD.UserEntry.FailedAccessTokenRemoved
FD.Enclave.TISStartAdminOp
FD.Enclave.OverrideDoorLockOK
FD.Enclave.TISUnlockDoorOp
FD.AuditLog.LogChange

CVS repository: test\UserEntry6.

3.11.1 Purpose

A user with a valid token attempts entry while the guard is logged on. The token does not contain an Auth certificate so biometric data should be requested. The user is slow providing this information so entry should be denied and no Auth cert written.

Additionally the guard overrides the door lock before the failed token has been removed. The user token is removed while the door is unlocked. This is done to check that the correct message appears on the display following the door being relocked.

Observe change in Stats, with a failed entry being logged.

3.11.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	-
	ConfigData	config data created by UpdateConfig1 test
	AdminToken	guard present (p02)

3.11.3 Test Procedure

Run test script and perform the requested actions.

This test requires a guard to be present, this can be achieved by running test Override1.

This test requires valid card with a no Auth Cert. The card information is held in **p05.dat**.

3.11.4 Expected Results

3.11.4.1 Audited Events

Id	Severity	User	Description
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
ScreenChanged	1	No User	SYSTEM BUSY PLEASE WAIT
UserTokenPresent	1	Issuer: 4294967295 SerialNo: 100000005	
AuthCertInvalid	1	Issuer: 4294967295 SerialNo: 100000005	
DisplayChanged	1	No User	AUTHENTICATING USER / INSERT FINGER
FingerTimeout	1	Issuer: 4294967295 SerialNo: 100000005	
DisplayChanged	1	No User	ENTRY DENIED / REMOVE TOKEN
ScreenChanged	1	No User	ENTER REQUIRED OPERATION
ScreenChanged	1	No User	PERFORMING OPERATION PLEASE WAIT
OperationStart	1	Issuer: 4294967295 SerialNo: 100000002	OVERRIDE
OverrideLock	1	Issuer: 4294967295 SerialNo: 100000002	
DisplayChanged	1	No User	/ ENTER ENCLAVE
LatchUnlocked	1	No User	
UserTokenRemoved	1	Issuer: 4294967295 SerialNo: 100000005	
DisplayChanged	1	No User	WELCOME TO TIS / ENTER TOKEN
LatchLocked	1	No User	

3.11.4.2 Keystore

keystore is unchanged.

3.11.4.3 Config data

Unchanged.

3.11.4.4 Visual

Screen Entity	Status
Door Alarm	OK throughout test
Audit Alarm	OK throughout test
Configuration Data	Never displayed.
System Stats	Always displayed, failed Entry should be increment by 1.
Messages	Values as detailed in audit log ScreenChanged entries.

3.12 UserEntry 7

ST.UserEntry.7.NoAuthFail

FD.UserEntry.TISReadUserToken
FD.UserEntry.BioCheckRequired
FD.UserEntry.ReadFingerOK
FD.UserEntry.ValidateFingerFail
FD.UserEntry.FailedAccessTokenRemoved
FD.AuditLog.LogChange

CVS repository: test\UserEntry7.

3.12.1 Purpose

A user with a valid token attempts entry while the guard is logged on. The token does not contain an Auth certificate so biometric data should be requested. The fingerprint provided does not match the I&A certificate so the entry is unsuccessful and no Auth Certificate is written.

Observe change in Stats, with a failed entry and failed bio check being logged.

3.12.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	-
	ConfigData	config data created by UpdateConfig1 test
	AdminToken	guard present (p02)

3.12.3 Test Procedure

Run test script and perform the requested actions.

This test requires a guard to be present, this can be achieved by running test Override1.

This test requires valid card with a no Auth Cert. The card information is held in UserEntry6/Temp/**p05.dat**.

3.12.4 Expected Results

3.12.4.1 Audited Events

Id	Severity	User	Description
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
ScreenChanged	1	No User	SYSTEM BUSY PLEASE WAIT
UserTokenPresent	1	Issuer: 4294967295 SerialNo: 100000005	
AuthCertInvalid	1	Issuer: 4294967295 SerialNo: 100000005	
DisplayChanged	1	No User	AUTHENTICATING USER / INSERT FINGER
FingerDetected	1	Issuer: 4294967295 SerialNo: 100000005	
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
FingerNotMatched	1	Issuer: 4294967295 SerialNo: 100000005	
DisplayChanged	1	No User	ENTRY DENIED / REMOVE TOKEN
ScreenChanged	1	No User	ENTER REQUIRED OPERATION
UserTokenRemoved	1	Issuer: 4294967295 SerialNo: 100000005	
DisplayChanged	1	No User	WELCOME TO TIS / ENTER TOKEN

3.12.4.2 Keystore

keystore is unchanged.

3.12.4.3 Config data

Unchanged.

3.12.4.4 Visual

Screen Entity	Status
Door Alarm	OK throughout test
Audit Alarm	OK throughout test
Configuration Data	Never displayed.
System Stats	Always displayed, failed Entry and failed Bio should be incremented by 1.
Messages	Values as detailed in audit log ScreenChanged entries.

3.13 UserEntry 8

ST.UserEntry.8.WithAuthSuccess

FD.UserEntry.TISReadUserToken
FD.UserEntry.BioCheckRequired
FD.UserEntry.ReadFingerOK
FD.UserEntry.ValidateFingerOK
FD.UserEntry.ConstructAuthCert
FD.UserEntry.WriteUserTokenOK
FD.UserEntry.WaitingTokenRemoval
FD.UserEntry.TokenRemovalTimeout
FD.Enclave.TISAdminLogout
FD.Enclave.AdminLogout
FD.AuditLog.LogChange

CVS repository: test\UserEntry8.

3.13.1 Purpose

Allow a user to acquire a valid Auth Certificate.

The user obtains a card with valid auth certificate. The user leaves their card in the reader too long after being requested to enter so the user entry times out.

The guard, who is present at the start of this operation, logs out during the operation.

3.13.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	-
	ConfigData	config data created by UpdateConfig1 test
	AdminToken	guard present (p02)

3.13.3 Test Procedure

Run test script and perform the requested actions.

This test requires a guard to be present, this can be achieved by running test Override1.

This test requires valid card with a no Auth Cert. The card information is held in UserEntry6/Temp/**p05.dat**.

The user does not go through the door at this point

3.13.4 Expected Results

3.13.4.1 Audited Events

Id	Severity	User	Description
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
ScreenChanged	1	No User	SYSTEM BUSY PLEASE WAIT
UserTokenPresent	1	Issuer: 4294967295 SerialNo: 100000005	
AuthCertInvalid	1	Issuer: 4294967295 SerialNo: 100000005	
DisplayChanged	1	No User	AUTHENTICATING USER / INSERT FINGER
FingerDetected	1	Issuer: 4294967295 SerialNo: 100000005	
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
AdminTokenRemoved	1	Issuer: 4294967295 SerialNo: 100000002	
FingerMatched	1	Issuer: 4294967295 SerialNo: 100000005	
AuthCertWritten	1	Issuer: 4294967295 SerialNo: 100000005	
EntryPermitted	1	Issuer: 4294967295 SerialNo: 100000005	
DisplayChanged	1	No User	/ REMOVE TOKEN AND ENTER
EntryTimeout	2	Issuer: 4294967295 SerialNo: 100000005	
DisplayChanged	1	No User	ENTRY DENIED / REMOVE TOKEN
ScreenChanged	1	No User	WELCOME TO TIS
UserTokenRemoved	1	Issuer: 4294967295 SerialNo: 100000005	
DisplayChanged	1	No User	WELCOME TO TIS / ENTER TOKEN

3.13.4.2 Keystore

keystore is unchanged.

3.13.4.3 Config data

Unchanged.

3.13.4.4 Visual

Screen Entity	Status
Door Alarm	OK throughout test
Audit Alarm	OK throughout test
Configuration Data	Never displayed.
System Stats	Displayed until the point at which the Screen message changes to "WELCOME TO TIS".
Messages	Values as detailed in audit log ScreenChanged entries.

3.14 UserEntry 9

ST.UserEntry.9.WithAuthSuccess

FD.Enclave.TISAdminLogin
FD.Enclave.GetPresentAdminToken
FD.Enclave.ValidateAdminTokenOK
FD.UserEntry.TISReadUserToken
FD.UserEntry.BioCheckNotRequired
FD.UserEntry.EntryOK
FD.AuditLog.LogChange
FD.Stats.Update

CVS repository: test\UserEntry9.

3.14.1 Purpose

Log-on the guard and then allow a user to enter the enclave without biometric checks.

This should allow monitoring of the Stats.

3.14.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	-
	ConfigData	config data created by UpdateConfig1 test

3.14.3 Test Procedure

Run test script and perform the requested actions.

This test requires the use of a Guard's card with an Auth Cert present. Such a card can be obtained by running test UserEntry2.

This test also requires the used a user's card with an Auth Cert present. Such a card can be obtained by running test UserEntry8.

3.14.4 Expected Results

3.14.4.1 Audited Events

Id	Severity	User	Description
AdminTokenPresent	1	Issuer: 4294967295 SerialNo: 100000002	
AdminTokenValid	1	Issuer: 4294967295 SerialNo: 100000002	
ScreenChanged	1	No User	ENTER REQUIRED OPERATION
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
ScreenChanged	1	No User	SYSTEM BUSY PLEASE WAIT
UserTokenPresent	1	Issuer: 4294967295 SerialNo: 100000005	
AuthCertValid	1	Issuer: 4294967295 SerialNo: 100000005	
EntryPermitted	1	Issuer: 4294967295 SerialNo: 100000005	
DisplayChanged	1	No User	/ REMOVE TOKEN AND ENTER
LatchUnlocked	1	No User	
DisplayChanged	1	No User	/ ENTER ENCLAVE
ScreenChanged	1	No User	ENTER REQUIRED OPERATION
DoorOpened	1	No User	
DoorClosed	1	No User	
LatchLocked	1	No User	
DisplayChanged	1	No User	WELCOME TO TIS / ENTER TOKEN
AdminTokeneRemoved	1	Issuer: 4294967295 SerialNo: 100000002	
ScreenChanged	1	No User	WELCOME TO TIS

3.14.4.2 Keystore

keystore is unchanged.

3.14.4.3 Config data

Unchanged.

3.14.4.4 Visual

Screen Entity	Status
Door Alarm	OK throughout test
Audit Alarm	OK throughout test
Configuration Data	Never displayed.
System Stats	Displayed once administrator is logged on. Increments successful entries by 1.
Messages	Values as detailed in audit log ScreenChanged entries.

3.15 AdminLogin 1

ST.AdminLogin.1.Fail

FD.Enclave.TISAdminLogin
FD.Enclave.ValidateAdminTokenFail
FD.Enclave.FailedAdminTokenRemoved
FD.AuditLog.LogChange

CVS repository: test\AdminLogin1.

3.15.1 Purpose

A user with no admin privileges attempts to logon as an Administrator. The user will not gain access to the administrator's console.

3.15.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	-
	ConfigData	config data created by UpdateConfig1 test

3.15.3 Test Procedure

Run test script and perform the requested actions.

This test requires the use of a user's card with an Auth Cert present. Such a card can be obtained by running test UserEntry8.

3.15.4 Expected Results

3.15.4.1 Audited Events

Id	Severity	User	Description
AdminTokenPresent	1	Issuer: 4294967295 SerialNo: 100000005	
AdminTokenInvalid	1	Issuer: 4294967295 SerialNo: 100000005	Authorisation Certificate not for Administrator
ScreenChanged	1	No User	REMOVE TOKEN
AdminTokenRemoved	1	Issuer: 4294967295 SerialNo: 100000005	
ScreenChanged	1	No User	WELCOME TO TIS

3.15.4.2 Keystore

keystore is unchanged.

3.15.4.3 Config data

Unchanged.

3.15.4.4 Visual

Screen Entity	**Status**
Door Alarm	OK throughout test
Audit Alarm	OK throughout test
Configuration Data	Never displayed.
System Stats	Never displayed.
Messages	Values as detailed in audit log ScreenChanged entries.

3.16 AdminLogin 2

ST.AdminLogin.2.Fail

FD.Enclave.TISAdminLogin
FD.Enclave.ValidateAdminTokenFail
FD.Enclave.FailedAdminTokenRemoved
FD.AuditLog.LogChange

CVS repository: test\AdminLogin2.

3.16.1 Purpose

An Audit Manager with no auth certificate on their token attempts to logon as an Administrator. The audit manager will not gain access to the administrators console.

3.16.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	-
	ConfigData	config data created by UpdateConfig1 test

3.16.3 Test Procedure

Run test script and perform the requested actions.

This test requires the use of a audit manager's card with no Auth Cert present. The card information is held in **p06.dat**

3.16.4 Expected Results

3.16.4.1 Audited Events

Id	Severity	User	Description
AdminTokenPresent	1	Issuer: 4294967295 SerialNo: 100000006	
AdminTokenInvalid	1	Issuer: 4294967295 SerialNo: 100000006	Authorisation Certificate bad
ScreenChanged	1	No User	REMOVE TOKEN
AdminTokenRemoved	1	Issuer: 4294967295 SerialNo: 100000006	
ScreenChanged	1	No User	WELCOME TO TIS

3.16.4.2 Keystore

keystore is unchanged.

3.16.4.3 Config data

Unchanged.

3.16.4.4 Visual

Screen Entity	**Status**
Door Alarm	OK throughout test
Audit Alarm	OK throughout test
Configuration Data	Never displayed.
System Stats	Never displayed.
Messages	Values as detailed in audit log ScreenChanged entries.

3.17 UserEntry 10

ST.UserEntry.10.NoAuthFail

FD.UserEntry.TISReadUserToken
FD.UserEntry.BioCheckRequired
FD.UserEntry.UserTokenTorn
FD.AuditLog.LogChange

CVS repository: test\UserEntry10.

3.17.1 Purpose

An administrator with role “Audit Manager” attempts entry but tears token before finger validation.

Entry will be denied.

3.17.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	-
	ConfigData	config data created by UpdateConfig1 test

3.17.3 Test Procedure

Run test script and perform the requested actions.

This test requires the use of a Audit manager’s card with no an Auth Cert present. The source for such a card is in AdminLogin2/Temp/**p06.dat**.

3.17.4 Expected Results

3.17.4.1 Audited Events

Id	Severity	User	Description
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
ScreenChanged	1	No User	SYSTEM BUSY PLEASE WAIT
UserTokenPresent	1	Issuer: 4294967295 SerialNo: 100000006	
AuthCertInvalid	1	Issuer: 4294967295 SerialNo: 100000006	
DisplayChanged	1	No User	AUTHENTICATING USER / INSERT FINGER
UserTokenRemoved	2	Issuer: 4294967295 SerialNo: 100000006	
DisplayChanged	1	No User	WELCOME TO TIS / ENTER TOKEN
ScreenChanged	1	No User	WELCOME TO TIS

3.17.4.2 Keystore

keystore is unchanged.

3.17.4.3 Config data

Unchanged.

3.17.4.4 Visual

Screen Entity	**Status**
Door Alarm	OK throughout test.
Audit Alarm	OK throughout test
Configuration Data	Never displayed.
System Stats	Never displayed.
Messages	Values as detailed in audit log ScreenChanged entries.

3.18 UserEntry 11

ST.UserEntry.11.NoAuthFail

FD.UserEntry.TISReadUserToken
FD.UserEntry.BioCheckRequired
FD.UserEntry.ReadFingerOK
FD.UserEntry.ValidateFingerOK
FD.UserEntry.UserTokenTorn
FD.AuditLog.LogChange

CVS repository: test\UserEntry11.

3.18.1 Purpose

An administrator with role “Audit Manager” attempts to enter the enclave biometric checks are required but the administrator removes token early during finger validation.

Entry is denied and no auth cert is written. (depending on timings of the test the auth cert may get written it is difficult to control the timing of the tear) however the tear should occur soon enough to prevent user entry.

3.18.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	-
	ConfigData	config data created by UpdateConfig1 test

3.18.3 Test Procedure

Run test script and perform the requested actions.

This test requires the use of a Audit manager’s card with no an Auth Cert present. The source for such a card is in AdminLogin2/Temp/**p06.dat**.

3.18.4 Expected Results

3.18.4.1 Audited Events

Id	Severity	User	Description
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
ScreenChanged	1	No User	SYSTEM BUSY PLEASE WAIT
UserTokenPresent	1	Issuer: 4294967295 SerialNo: 100000006	
AuthCertInvalid	1	Issuer: 4294967295 SerialNo: 100000006	
DisplayChanged	1	No User	AUTHENTICATING USER / INSERT FINGER
FingerDetected	1	Issuer: 4294967295 SerialNo: 100000006	
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
FingerMatched	1	Issuer: 4294967295 SerialNo: 100000006	
UserTokenRemoved	2	Issuer: 4294967295 SerialNo: 100000006	
DisplayChanged	1	No User	WELCOME TO TIS / ENTER TOKEN
ScreenChanged	1	No User	WELCOME TO TIS

3.18.4.2 Keystore

keystore is unchanged.

3.18.4.3 Config data

Unchanged.

3.18.4.4 Visual

Screen Entity	Status
Door Alarm	OK throughout test
Audit Alarm	OK throughout test
Configuration Data	Never displayed.
System Stats	Never displayed.
Messages	Values as detailed in audit log ScreenChanged entries.

3.19 UserEntry 12

ST.UserEntry.12.NoAuthSuccess

FD.UserEntry.TISReadUserToken
FD.UserEntry.BioCheckRequired
FD.UserEntry.ReadFingerOK
FD.UserEntry.ValidateFingerOK
FD.UserEntry.ConstructAuthCert
FD.UserEntry.WriteUserTokenOK
FD.UserEntry.EntryOK
FD.AuditLog.LogChange

CVS repository: test\UserEntry12.

3.19.1 Purpose

Allow an administrator with role “Audit Manager” to enter the enclave following biometric checks.

The door is forced open during the user entry causing an alarm to be momentarily raised.

3.19.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	-
	ConfigData	config data created by UpdateConfig1 test

3.19.3 Test Procedure

Run test script and perform the requested actions.

This test requires the use of a Audit manager’s card with no an Auth Cert present. The source for such a card is in AdminLogin2/Temp/**p06.dat**.

3.19.4 Expected Results

3.19.4.1 Audited Events

Id	Severity	User	Description
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
ScreenChanged	1	No User	SYSTEM BUSY PLEASE WAIT
UserTokenPresent	1	Issuer: 4294967295 SerialNo: 100000006	
AuthCertInvalid	1	Issuer: 4294967295 SerialNo: 100000006	
DisplayChanged	1	No User	AUTHENTICATING USER / INSERT FINGER
FingerDetected	1	Issuer: 4294967295 SerialNo: 100000006	
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
DoorOpened	1	No User	
AlarmRaised	3	No User	
FingerMatched	1	Issuer: 4294967295 SerialNo: 100000006	
AuthCertWritten	1	Issuer: 4294967295 SerialNo: 100000006	
EntryPermitted	1	Issuer: 4294967295 SerialNo: 100000006	
DisplayChanged	1	No User	/ REMOVE TOKEN AND ENTER
LatchUnlocked	1	No User	
AlarmSilenced	1	No User	
DisplayChanged	1	No User	/ ENTER ENCLAVE
ScreenChanged	1	No User	WELCOME TO TIS
DoorClosed	1	No User	
LatchLocked	1	No User	
DisplayChanged	1	No User	WELCOME TO TIS / ENTER TOKEN

3.19.4.2 Keystore

keystore is unchanged.

3.19.4.3 Config data

Unchanged.

3.19.4.4 Visual

Screen Entity	Status
Door Alarm	OK until user holds door forced open. Then raised and cleared a seconds later when the latch is released to allow entry to validated user door is closed.
Audit Alarm	OK throughout test
Configuration Data	Never displayed.
System Stats	Never displayed.
Messages	Values as detailed in audit log ScreenChanged entries.

3.20 UpdateConfig 2

ST.UpdateConfig.2.Fail

FD.Enclave.TISAdminLogin
FD.Enclave.GetPresentAdminToken
FD.Enclave.ValidateAdminTokenOK
FD.Enclave.TISStartAdminOp
FD.Enclave.ValidateOpRequestOK
FD.Enclave.StartUpdateConfigDataWaitingFloppy
FD.Enclave.StartUpdateConfigDataOK
FD.Enclave.FinishUpdateConfigDataFail
FD.AuditLog.LogChange

CVS repository: test\UpdateConfig2.

3.20.1 Purpose

Logon a Security Officer and attempt to change the configuration data to invalid data.

Update of the configuration data will not take place.

3.20.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	-
	ConfigData	config data created by UpdateConfig1 test

3.20.3 Test Procedure

Run test script and perform the requested actions.

This test requires the use of a Security Officer's card with a current Auth Cert present. Such a card can be obtained by running test UserEntry1.

3.20.4 Expected Results

3.20.4.1 Audited Events

Id	Severity	User	Description
AdminTokenPresent	1	Issuer: 4294967295 SerialNo: 100000001	
AdminTokenValid	1	Issuer: 4294967295 SerialNo: 100000001	
ScreenChanged	1	No User	ENTER REQUIRED OPERATION
ScreenChanged	1	No User	PERFORMING OPERATION PLEASE WAIT
OperationStart	1	Issuer: 4294967295 SerialNo: 100000001	UPDATE CONFIG
ScreenChanged	1	No User	INSERT CONFIGURATION DATA FLOPPY
ScreenChanged	1	No User	PERFORMING OPERATION PLEASE WAIT
InvalidConfigData	1	Issuer: 4294967295 SerialNo: 100000001	
ScreenChanged	1	No User	INVALID DATA: PLEASE ENTER NEW OPERATION

3.20.4.2 Keystore

keystore is unchanged.

3.20.4.3 Config data

Unchanged.

3.20.4.4 Visual

Screen Entity	Status
Door Alarm	OK until user holds door open too long. Then raised and cleared a few seconds later when door is closed.
Audit Alarm	OK throughout test
Configuration Data	Never displayed.
System Stats	Never displayed.
Messages	Values as detailed in audit log ScreenChanged entries.

3.21 UpdateConfig 3

ST.UpdateConfig.3.Success

FD.Enclave.TISStartAdminOp
FD.Enclave.ValidateOpRequestOK
FD.Enclave.StartUpdateConfigDataWaitingFloppy
FD.Enclave.StartUpdateConfigDataOK
FD.Enclave.FinishUpdateConfigDataOK
FD.Enclave.TISAdminLogout
FD.Enclave.AdminLogout
FD.AuditLog.LogChange

CVS repository: test\UpdateConfig3.

3.21.1 Purpose

Update the configuration data to an all hours configuration with very short validity period.

The administrator with Security Officer role is already logged on following test Config2.

Finally the Admin token is removed to log out the administrator.

3.21.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	Empty
	ConfigData	config.dat created by Config1 test
	AdminToken	Security officer present (p01)

3.21.3 Test Procedure

Run test script and perform the requested actions.

This test requires the use of an administrator's card. The card used is the card used for the test UserEntry1, which should contain an auth certificate following successful execution of UserEntry1.

This test also requires the use of new config data supplied on a floppy.

3.21.4 Expected Results

3.21.4.1 Audited Events

Id	Severity	User	Description
OperationStart	1	Issuer: 4294967295 SerialNo: 100000001	UPDATE CONFIG
ScreenChanged	1	No User	PERFORMING OPERATION PLEASE WAIT
UpdatedConfigData	1	Issuer: 4294967295 SerialNo: 100000001	20; 30; 15; 100; TOPSECRET; 07:30; 16:45; 00:05; ALLHOURS; SECRET; 1000; 260; 1500
ScreenChanged	1	No User	ENTER REQUIRED OPERATION
AdminTokenRemoved	1	Issuer: 4294967295 SerialNo: 100000001	
ScreenChanged	1	No User	WELCOME TO TIS

3.21.4.2 Keystore

keystore is unchanged.

3.21.4.3 Config data

Changed, the file System/config.dat should have the same contents as the file provided on floppy.

3.21.4.4 Visual

Screen Entity	**Status**
Door Alarm	OK throughout test
Audit Alarm	OK throughout test
Configuration Data	Displayed while SecurityOfficer logged on and changes to match supplied config file.
System Stats	Displayed while Admin logged on.
Messages	values as detailed in audit log ScreenChanged entries.

3.22 AdminLogout 1

ST.AdminLogout.1.TimeoutSuccess

FD.UserEntry.TISReadUserToken
FD.UserEntry.BioCheckRequired
FD.UserEntry.ReadFingerOK
FD.UserEntry.ValidateFingerOK
FD.UserEntry.ConstructAuthCert
FD.UserEntry.WriteUserTokenOK
FD.UserEntry.EntryOK
FD.UserEntry.UnlockDoorOK
FD.Enclave.GetPresentAdminToken
FD.Enclave.ValidateAdminTokenOK
FD.Enclave.AdminTokenTimeout
FD.Enclave.TISCompleteTimeoutAdminLogout
FD.AuditLog.LogChange

CVS repository: test\AdminLogout1.

3.22.1 Purpose

Allow an administrator with role “Guard” to enter the enclave and acquire a valid Auth Certificate, which will be used to check that the guard login is timed out 5 minutes after it entered the enclave.

The administrator enters the enclave successfully and obtains a card with valid auth certificate.

The administrator logs on as a guard and waits. After approx 5 minutes the guard will be automatically logged off.

3.22.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	-
	ConfigData	config.dat created by Config3 test

3.22.3 Test Procedure

Run test script and perform the requested actions.

This test requires the use of a Guard’s card with no Auth Cert present. The source for this card is **p07**.

3.22.4 Expected Results

3.22.4.1 Audited Events

Id	Severity	User	Description
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
ScreenChanged	1	No User	SYSTEM BUSY PLEASE WAIT
UserTokenPresent	1	Issuer: 4294967295 SerialNo: 100000007	
AuthCertInvalid	1	Issuer: 4294967295 SerialNo: 100000007	
DisplayChanged	1	No User	AUTHENTICATING USER / INSERT FINGER
FingerDetected	1	Issuer: 4294967295 SerialNo: 100000007	
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
FingerMatched	1	Issuer: 4294967295 SerialNo: 100000007	
AuthCertWritten	1	Issuer: 4294967295 SerialNo: 100000007	
EntryPermitted	1	Issuer: 4294967295 SerialNo: 100000007	
DisplayChanged	1	No User	/ REMOVE TOKEN AND ENTER
DisplayChanged	1	No User	/ ENTER ENCLAVE
ScreenChanged	1	No User	WELCOME TO TIS
LatchUnlocked	1	No User	
DoorOpened	1	No User	
DoorClosed	1	No User	
LatchLocked	1	No User	
DisplayChanged	1	No User	WELCOME TO TIS / ENTER TOKEN
AdminTokenPresent	1	Issuer: 4294967295 SerialNo: 100000007	
AdminTokenValid	1	Issuer: 4294967295 SerialNo: 100000007	
ScreenChanged	1	No User	ENTER REQUIRED OPERATION

AdminTokenExpired	2	Issuer: 4294967295 SerialNo: 100000007	
ScreenChanged	1	No User	REMOVE TOKEN
AdminTokenRemoved	1	Issuer: 4294967295 SerialNo: 100000007	
ScreenChanged	1	No User	WELCOME TO TIS

3.22.4.2 Keystore

keystore is unchanged.

3.22.4.3 Config data

Unchanged.

3.22.4.4 Visual

Screen Entity	Status
Door Alarm	OK throughout test
Audit Alarm	OK throughout test
Configuration Data	Never displayed.
System Stats	Displayed for approx 5 minutes while guard is logged on.
Messages	Values as detailed in audit log ScreenChanged entries.

3.23 AdminLogin 3

ST.AdminLogin.3.ExpiredFail

FD.Enclave.GetPresentAdminToken
FD.Enclave.ValidateAdminTokenFailed
FD.Enclave.AdminLogout
FD.AuditLog.LogChange

CVS repository: test\AdminLogin3.

3.23.1 Purpose

Guard attempts to login as administrator after their token has expired.

The Guard is not logged on to the system.

3.23.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	-
	ConfigData	config.dat created by Config3 test

3.23.3 Test Procedure

Run test script and perform the requested actions.

This test requires the use of a Guard's card with expired Auth Cert present. This can be obtained by running test AdminLogout1.

3.23.4 Expected Results

3.23.4.1 Audited Events

Id	Severity	User	Description
AdminTokenPresent	1	Issuer: 4294967295 SerialNo: 100000007	
AdminTokenInvalid	1	Issuer: 4294967295 SerialNo: 100000007	Authorisation Certificate Not Current
ScreenChanged	1	No User	REMOVE TOKEN
AdminTokenRemoved	1	Issuer: 4294967295 SerialNo: 100000007	
ScreenChanged	1	No User	WELCOME TO TIS

3.23.4.2 Keystore

keystore is unchanged.

3.23.4.3 Config data

Unchanged.

3.23.4.4 Visual

Screen Entity	**Status**
Door Alarm	OK throughout test
Audit Alarm	OK throughout test
Configuration Data	Never displayed.
System Stats	Never displayed
Messages	Values as detailed in audit log ScreenChanged entries.

3.24 UpdateConfig 4

ST.UpdateConfig.4.Fail

FD.Enclave.TISStartAdminOp
FD.Enclave.ValidateOpRequestOK
FD.Enclave.StartUpdateConfigDataWaitingFloppy
FD.Enclave.BadAdminLogout
FD.Enclave.TISAdminLogout
FD.AuditLog.LogChange

CVS repository: test\UpdateConfig4.

3.24.1 Purpose

Security officer starts an update configuration data operation but removes his card before the operation can complete.

The configuration data is not updated.

3.24.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	Empty
	ConfigData	config.dat created by Config3 test

3.24.3 Test Procedure

Run test script and perform the requested actions.

This test requires the use of an administrator's card. The card used is the card used for the test UserEntry1, which should contain an auth certificate following successful execution of UserEntry1.

This test also requires the use of new config data supplied on a floppy.

3.24.4 Expected Results

3.24.4.1 Audited Events

Id	Severity	User	Description
AdminTokenPresent	1	Issuer: 4294967295 SerialNo: 100000001	
AdminTokenValid	1	Issuer: 4294967295 SerialNo: 100000001	
ScreenChanged	1	No User	ENTER REQUIRED OPERATION
ScreenChanged	1	No User	PERFORMING OPERATION PLEASE WAIT
OperationStart	1	Issuer: 4294967295 SerialNo: 100000001	UPDATE CONFIG
ScreenChanged	1	No User	INSERT CONFIGURATION DATA FLOPPY
AdminTokenRemoved	2	Issuer: 4294967295 SerialNo: 100000001	
ScreenChanged	1	No User	WELCOME TO TIS

3.24.4.2 Keystore

keystore is unchanged.

3.24.4.3 Config data

Unchanged.

3.24.4.4 Visual

Screen Entity	**Status**
Door Alarm	OK throughout test
Audit Alarm	OK throughout test
Configuration Data	Displayed while SecurityOfficer logged on.
System Stats	Displayed while Admin logged on.
Messages	values as detailed in audit log ScreenChanged entries.

3.25 UpdateConfig 5

ST.UpdateConfig.5.Success

FD.Enclave.TISStartAdminOp
FD.Enclave.ValidateOpRequestOK
FD.Enclave.StartUpdateConfigDataOK
FD.Enclave.FinishUpdateConfigDataOK
FD.AuditLog.LogChange

CVS repository: test\UpdateConfig5.

3.25.1 Purpose

Update the configuration data to a working hours configuration with long times for latch unlock duration.

3.25.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	Empty
	ConfigData	config.dat created by Config3 test

3.25.3 Test Procedure

Run test script and perform the requested actions.

This test requires the use of an administrator's card. The card used is the card used for the test UserEntry1, which should contain an auth certificate following successful execution of UserEntry1.

This test also requires the use of newconfig data supplied on a floppy.

3.25.4 Expected Results

3.25.4.1 Audited Events

Id	Severity	User	Description
AdminTokenPresent	1	Issuer: 4294967295 SerialNo: 100000001	
AdminTokenValid	1	Issuer: 4294967295 SerialNo: 100000001	
ScreenChanged	1	No User	ENTER REQUIRED OPERATION
ScreenChanged	1	No User	PERFORMING OPERATION PLEASE WAIT
OperationStart	1	Issuer: 4294967295 SerialNo: 100000001	UPDATE CONFIG
ScreenChanged	1	No User	INSERT CONFIGURATION DATA FLOPPY
ScreenChanged	1	No User	PERFORMING OPERATION PLEASE WAIT
UpdatedConfigData	1	Issuer: 4294967295 SerialNo: 100000001	40; 200; 20; 100; SECRET; 08:30; 17:45; 00:05; WORKINGHOURS; RESTRICTED; 1000; 260; 1500
ScreenChanged	1	No User	ENTER REQUIRED OPERATION

3.25.4.2 Keystore

keystore is unchanged.

3.25.4.3 Config data

Changed, the file System/config.dat should have the same contents as the file provided on floppy.

3.25.4.4 Visual

Screen Entity	Status
Door Alarm	OK throughout test
Audit Alarm	OK throughout test
Configuration Data	Displayed while SecurityOfficer logged on and changes to match supplied config file.
System Stats	Displayed while Admin logged on.
Messages	values as detailed in audit log ScreenChanged entries.

3.26 Shutdown 1

ST.Shutdown.1.Success

FD.UserEntry.TISReadUserToken
FD.UserEntry.BioCheckNotRequired
FD.UserEntry.EntryOK
FD.Enclave.ValidateOpRequestOK
FD.Enclave.ShutdownWaitingDoor
FD.Enclave.TIS.ShutDownOp
FD.Enclave.ShutdownOK
FD.AuditLog.LogChange

CVS repository: test\Shutdown1.

3.26.1 Purpose

A user enters the enclave and before the door is closed the Security officer performs a shutdown operation.

The system waits for the door to be closed before shutting down. The admin token is removed before the door is shut but this should not impact the success of the operation.

3.26.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	-
	ConfigData	config data created by UpdateConfig5 test
	AdminToken	security officer present (p07)

3.26.3 Test Procedure

Run test script and perform the requested actions.

This test requires the use of a Audit Manager's card with an Auth Cert present. Such a card can be obtained by running test UserEntry12.

This test also requires the security officer to be present before the test is run. This can be achieved by running test Config5.

3.26.4 Expected Results

3.26.4.1 Audited Events

Id	Severity	User	Description
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
ScreenChanged	1	No User	SYSTEM BUSY PLEASE WAIT
UserTokenPresent	1	Issuer: 4294967295 SerialNo: 100000006	
AuthCertValid	1	Issuer: 4294967295 SerialNo: 100000006	
EntryPermitted	1	Issuer: 4294967295 SerialNo: 100000006	
DisplayChanged	1	No User	/ REMOVE TOKEN AND ENTER
LatchUnlocked	1	No User	
DisplayChanged	1	No User	/ ENTER ENCLAVE
ScreenChanged	1	No User	ENTER REQUIRED OPERATION
DoorOpened	1	No User	
ScreenChanged	1	No User	PERFORMING OPERATION PLEASE WAIT
OperationStart	1	Issuer: 4294967295 SerialNo: 100000001	SHUTDOWN
ScreenChanged	1	No User	CLOSE ENCLAVE DOOR
DoorClosed	1	No User	
ScreenChanged	1	No User	PERFORMING OPERATION PLEASE WAIT
DisplayChanged	1	NoUser	SYSTEM NOT OPERATIONAL /
LatchLocked	1	NoUser	
Shutdown	1	Issuer: 4294967295 SerialNo: 100000001	

3.26.4.2 Keystore

keystore is unchanged.

3.26.4.3 Config data

Unchanged.

3.26.4.4 Visual

Screen Entity	Status
Door Alarm	OK until user holds door open too long. Then raised and cleared a few seconds later when door is closed.
Audit Alarm	OK throughout test
Configuration Data	Never displayed.
System Stats	Never displayed.
Messages	Values as detailed in audit log ScreenChanged entries.

3.27 ArchiveLog 1

ST.ArchiveLog.1.FailFloppyRemoved

FD.TIS.TISStartup
FD.Enclave.TISAdminLogin
FD.Enclave.GetPresentAdminToken
FD.Enclave.ValidateAdminTokenOK
FD.Enclave.TISStartAdminOp
FD.Enclave.ValidateOpRequestOK
FD.Enclave.StartArchiveLogWaitingFloppy
FD.Enclave.StartArchiveLogOK
FD.Enclave.FinishArchiveLogNoFloppy
FD.Enclave.TISArchiveLogOp
FD.AuditLog.LogChange

CVS repository: test\ArchiveLog1.

3.27.1 Purpose

Allow an administrator with role “Audit Manager” to log on and start an archive activity.

The archive will be made to fail by removing the floppy from the drive before the archive has been checked.

3.27.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	Log supplied in Temp directory.
	ConfigData	config data created by UpdateConfig5 test

3.27.3 Test Procedure

Run test script and perform the requested actions.

This test requires the use of a Audit Manager’s card with an Auth Cert present. Such a card can be obtained by running test UserEntry12.

3.27.4 Expected Results

3.27.4.1 Audited Events

Id	Severity	User	Description
StartEnrolledTIS	1	No User	-
AdminTokenPresent	1	Issuer: 4294967295 SerialNo: 100000006	
AdminTokenValid	1	Issuer: 4294967295 SerialNo: 100000006	
ScreenChanged	1	No User	ENTER REQUIRED OPERATION
ScreenChanged	1	No User	PERFORMING OPERATION PLEASE WAIT
OperationStart	1	Issuer: 4294967295 SerialNo: 100000006	ARCHIVE
ScreenChanged	1	No User	INSERT BLANK FLOPPY
ArchiveLog	1	Issuer: 4294967295 SerialNo: 100000006	From: 2003-08-12 14:09:23.3 to: 2003-08-12 14:13:09.7
ScreenChanged	1	No User	PERFORMING OPERATION PLEASE WAIT
ArchiveCheckFailed	2	Issuer: 4294967295 SerialNo: 100000006	Archive Cancelled - Floppy has been removed
ScreenChanged	1	No User	ARCHIVE FAILED: PLEASE ENTER NEW OPERATION

3.27.4.2 Keystore

keystore is unchanged.

3.27.4.3 Config data

Unchanged.

3.27.4.4 Visual

Screen Entity	Status
Door Alarm	OK throughout test.
Audit Alarm	Initially OK, but raised as soon as system logs startup.
Configuration Data	Never displayed.
System Stats	Displayed once Audit Manager is logged on.
Messages	Values as detailed in audit log ScreenChanged entries.

3.28 ArchiveLog 2

ST.ArchiveLog.2.FailBadFloppy

FD.Enclave.ValidateOpRequestOK
FD.Enclave.StartArchiveLogWaitingFloppy
FD.Enclave.StartArchiveLogOK
FD.Enclave.FinishArchiveLogBadMatch
FD.Enclave.TISArchiveLogOp
FD.AuditLog.LogChange

CVS repository: test\ArchiveLog2.

3.28.1 Purpose

Allow an administrator with role “Audit Manager” to start an archive activity.

The archive will be made to fail by providing a floppy which already contains a non-matching archive.

3.28.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	Log created by AuditLog1 test.
	ConfigData	config data created by UpdateConfig5 test
	AdminToken	Audit Manager present (p06)

3.28.3 Test Procedure

Run test script and perform the requested actions.

This test requires an audit manager to be present, this can be achieved by running test ArchiveLog1.

3.28.4 Expected Results

3.28.4.1 Audited Events

Id	Severity	User	Description
ScreenChanged	1	No User	PERFORMING OPERATION PLEASE WAIT
OperationStart	1	Issuer: 4294967295 SerialNo: 100000006	ARCHIVE
ArchiveLog	1	Issuer: 4294967295 SerialNo: 100000006	From: 2003-08-12 14:09:23.3 to: 2003-08-12 14:13:09.7
ArchiveCheckFailed	2	Issuer: 4294967295 SerialNo: 100000006	Archive Cancelled - Floppy has bad data
ScreenChanged	1	No User	ARCHIVE FAILED: PLEASE ENTER NEW OPERATION

3.28.4.2 Keystore

keystore is unchanged.

3.28.4.3 Config data

Unchanged.

3.28.4.4 Visual

Screen Entity	**Status**
Door Alarm	OK throughout test.
Audit Alarm	Failed throughout test.
Configuration Data	Never displayed.
System Stats	Displayed throughout – no change.
Messages	Values as detailed in audit log ScreenChanged entries.

3.29 ArchiveLog 3

ST.ArchiveLog.3.Success

FD.Enclave.ValidateOpRequestOK
FD.Enclave.StartArchiveLogWaitingFloppy
FD.Enclave.StartArchiveLogOK
FD.Enclave.FinishArchiveLogOK
FD.Enclave.TISArchiveLogOp
FD.Enclave.TISAdminLogout
FD.Enclave.AdminLogout
FD.AuditLog.LogChange

CVS repository: test\ArchiveLog3.

3.29.1 Purpose

Allow an administrator with role “Audit Manager” to perform a successful archive log activity.

This should result in the audit alarm being cleared.

At the end of the test the audit manager is logged out.

3.29.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	Log created by AuditLog2 test.
	ConfigData	config data created by UpdateConfig5 test
	AdminToken	Audit Manager present (p06)

3.29.3 Test Procedure

Run test script and perform the requested actions.

This test requires an audit manager to be present, this can be achieved by running test ArchiveLog1.

3.29.4 Expected Results

3.29.4.1 Audited Events

Id	Severity	User	Description
ScreenChanged	1	No User	PERFORMING OPERATION PLEASE WAIT
OperationStart	1	Issuer: 4294967295 SerialNo: 100000006	ARCHIVE
ArchiveLog	1	Issuer: 4294967295 SerialNo: 100000006	From : 2003-08-12 14:09:23.3 To : 2003-08-12 14:13:09.7
AuditAlarmSilenced	1	No User	
ArchiveComplete	1	Issuer: 4294967295 SerialNo: 100000006	
ScreenChanged	1	No User	ENTER REQUIRED OPERATION
AdminTokenRemoved	1	Issuer: 4294967295 SerialNo: 100000006	
ScreenChanged	1	No User	WELCOME TO TIS

3.29.4.2 Keystore

keystore is unchanged.

3.29.4.3 Config data

Unchanged.

3.29.4.4 Visual

Screen Entity	Status
Door Alarm	OK throughout test.
Audit Alarm	Failed at start of test, OK once archive complete.
Configuration Data	Never displayed.
System Stats	Displayed throughout until Audit manager logs out at end of test.
Messages	Values as detailed in audit log ScreenChanged entries.

3.30 UserEntry 13

ST.UserEntry.13.WriteAuthFailEntryOK

FD.UserEntry.TISReadUserToken
FD.UserEntry.BioCheckRequired
FD.UserEntry.ReadFingerOK
FD.UserEntry.ValidateFingerOK
FD.UserEntry.WriteUserTokenFail
FD.UserEntry.EntryOK
FD.UserEntry.UnlockDoorOK
FD.AuditLog.LogChange

CVS repository: test\UserEntry13.

3.30.1 Purpose

A user provides a valid token for entry but there is a system failure when signing the Auth Certificate so the certificate is not written.

The user still gains entry to the enclave.

3.30.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	-
	ConfigData	config data created by UpdateConfig5 test

3.30.3 Test Procedure

Run test script and perform the requested actions.

This test requires the use of a User's card with no Auth Cert present. The source for such a card is in UserEntry13/Temp/**p07.dat**.

3.30.4 Expected Results

3.30.4.1 Audited Events

Id	Severity	User	Description
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
ScreenChanged	1	No User	SYSTEM BUSY PLEASE WAIT
UserTokenPresent	1	Issuer: 4294967295 SerialNo: 100000007	
AuthCertInvalid	1	Issuer: 4294967295 SerialNo: 100000007	
DisplayChanged	1	No User	AUTHENTICATING USER / INSERT FINGER
FingerDetected	1	Issuer: 4294967295 SerialNo: 100000007	
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
FingerMatched	1	Issuer: 4294967295 SerialNo: 100000007	
SystemFault	2		Crypto Library Error in Sign : DEVICEERROR
AuthCertWriteFailed	1	Issuer: 4294967295 SerialNo: 100000007	
DisplayChanged	1	No User	/ TOKEN UPDATE FAILED
EntryPermitted	1	Issuer: 4294967295 SerialNo: 100000006	
DisplayChanged	1	No User	/ REMOVE TOKEN AND ENTER
LatchUnlocked	1	No User	
DisplayChanged	1	No User	/ ENTER ENCLAVE
ScreenChanged	1	No User	WELCOME TO TIS
DoorOpened	1	No User	
DoorClosed	1	No User	
LatchLocked	1	No User	
DisplayChanged	1	No User	WELCOME TO TIS / ENTER TOKEN

3.30.4.2 Keystore

keystore is unchanged.

3.30.4.3 Config data

Unchanged.

3.30.4.4 Visual

Screen Entity	Status
Door Alarm	OK throughout test
Audit Alarm	OK throughout test
Configuration Data	Never displayed.
System Stats	Never displayed.
Messages	Values as detailed in audit log ScreenChanged entries.

3.31 UserEntry 14

ST.UserEntry.14.WriteAuthAndEntryFailed

FD.Enclave.TISAdminLogin
FD.Enclave.GetPresentAdminToken
FD.Enclave.ValidateAdminTokenOK
FD.Enclave.TISStartAdminOp
FD.Enclave.ValidateOpRequestOK
FD.Enclave.StartUpdateConfigDataOK
FD.Enclave.FinishUpdateConfigDataOK
FD.UserEntry.TISReadUserToken
FD.UserEntry.BioCheckRequired
FD.UserEntry.ReadFingerOK
FD.UserEntry.ValidateFingerOK
FD.UserEntry.WriteUserTokenFail
FD.UserEntry.FailedAccessTokenRemoved
FD.Enclave.TISAdminLogout
FD.Enclave.AdminLogout
FD.AuditLog.LogChange

CVS repository: test\UserEntry14.

3.31.1 Purpose

A security officer logs on and changes the configuration data so that working hours are only late at night.

A user then attempts entry with a valid token but the signing fails and the Auth Certificate is not written. The user is denied entry since the current time is not within the entry times.

The security officer then logs off.

3.31.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	-
	ConfigData	config data created by UpdateConfig5 test

3.31.3 Test Procedure

Run test script and perform the requested actions.

This test requires the use of a Security Officer's card with an Auth Cert present, such a card can be generated by running test UserEntry1.

This test requires the use of a User's card with no Auth Cert present. The source for such a card is in UserEntry13/Temp/**p07.dat**.

3.31.4 Expected Results

3.31.4.1 Audited Events

Id	Severity	User	Description
AdminTokenPresent	1	Issuer: 4294967295 SerialNo: 100000001	
AdminTokenValid	1	Issuer: 4294967295 SerialNo: 100000001	
ScreenChanged	1	No User	ENTER REQUIRED OPERATION
ScreenChanged	1	No User	PERFORMING OPERATION PLEASE WAIT
OperationStart	1	Issuer: 4294967295 SerialNo: 100000001	UPDATE CONFIG
UpdatedConfigData	1	Issuer: 4294967295 SerialNo: 100000001	20; 30; 15; 20; RESTRICTED; 20:30; 23:45; 02:00; WORKINGHOURS; UNCLASSIFIED; 1000; 260; 1000
ScreenChanged	1	No User	ENTER REQUIRED OPERATION
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
ScreenChanged	1	No User	SYSTEM BUSY PLEASE WAIT
UserTokenPresent	1	Issuer: 4294967295 SerialNo: 100000007	
AuthCertInvalid	1	Issuer: 4294967295 SerialNo: 100000007	
DisplayChanged	1	No User	AUTHENTICATING USER / INSERT FINGER
FingerDetected	1	Issuer: 4294967295 SerialNo: 100000007	
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
FingerMatched	1	Issuer: 4294967295 SerialNo: 100000006	
SystemFault	2		Crypto Library Error in Sign : DEVICEERROR
AuthCertWriteFailed	1	Issuer: 4294967295 SerialNo: 100000007	
DisplayChanged	1	No User	/ TOKEN UPDATE FAILED
EntryDenied	1	Issuer: 4294967295	

		SerialNo: 100000007	
DisplayChanged	1	No User	ENTRY DENIED / REMOVE TOKEN
ScreenChanged	1	No User	ENTER REQUIRED OPERATION
UserTokenRemoved	1	Issuer: 4294967295 SerialNo: 100000007	
DisplayChanged	1	No User	WELCOME TO TIS / ENTER TOKEN
AdminTokenRemoved	1	Issuer: 4294967295 SerialNo: 100000001	
ScreenChanged	1	No User	WELCOME TO TIS

3.31.4.2 Keystore

keystore is unchanged.

3.31.4.3 Config data

Changed, the file System/config.dat should have the same contents as the file provided on floppy.

3.31.4.4 Visual

Screen Entity	Status
Door Alarm	OK throughout test
Audit Alarm	OK throughout test
Configuration Data	Displayed while security officer is logged on.
System Stats	Displayed while security officer is logged on.
Messages	Values as detailed in audit log ScreenChanged entries.

3.32 Shutdown 2

ST.Shutdown.2.Success

FD.Enclave.GetPresentAdminToken
FD.Enclave.ValidateAdminTokenOK
FD.Enclave.TISStartAdminOp
FD.Enclave.ValidateOpRequestOK
FD.Enclave.TISShutDownOp
FD.Enclave.ShutdownOK
FD.AuditLog.LogChange

CVS repository: test\Shutdown2.

3.32.1 Purpose

The Security officer logs on and performs a shutdown operation.

The system is shutdown as soon as the operation is received, as the door is already closed.

3.32.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	-
	ConfigData	config data created by UpdateConfig5 test
	AdminToken	security officer present (p07)

3.32.3 Test Procedure

Run test script and perform the requested actions.

This test also requires the use of a security officer's card with an Auth Cert present. Such a card can be obtained by running test UserEntry1.

3.32.4 Expected Results

3.32.4.1 Audited Events

Id	Severity	User	Description
AdminTokenPresent	1	Issuer: 4294967295 SerialNo: 100000001	
AdminTokenValid	1	Issuer: 4294967295 SerialNo: 100000001	
ScreenChanged	1	No User	ENTER REQUIRED OPERATION
ScreenChanged	1	No User	PERFORMING OPERATION PLEASE WAIT
OperationStart	1	Issuer: 4294967295 SerialNo: 100000001	SHUTDOWN
ScreenChanged	1	No User	
DisplayChanged	1	No User	/ SYSTEM NOT OPERATIONAL
Shutdown	1	Issuer: 4294967295 SerialNo: 100000001	

3.32.4.2 Keystore

keystore is unchanged.

3.32.4.3 Config data

Unchanged.

3.32.4.4 Visual

Screen Entity	**Status**
Door Alarm	OK throughout test
Audit Alarm	Failed throughout test
Configuration Data	Never displayed.
System Stats	Never displayed.
Messages	Values as detailed in audit log ScreenChanged entries.

3.33 TruncateLog 1

ST.TruncateLog.1.Success

FD.AuditLog.AddElementToLogFile
FD.AuditLog.TruncateLog
FD.AuditLog.AddElementToLog
FD.AuditLog.AddElementsToLog
FD.AuditLog.LogChange

CVS repository: test\TruncateLog1.

3.33.1 Purpose

The system is started with only 3 more spaces in the final log file. Sufficient actions are performed to ensure that the final log file is filled and the log is truncated.

3.33.2 Initial State

	Entity	State
TIS persistent state	Keystore	keystore created by Enrol3 test
	AuditLog	Log supplied in Temp directory
	ConfigData	config data created by UpdateConfig5 test

3.33.3 Test Procedure

Run test script and perform the requested actions.

3.33.4 Expected Results

3.33.4.1 Audited Events

Id	Severity	User	Description
StartEnrolledTIS	1	No User	-
DisplayChanged	1	No User	AUTHENTICATING USER / PLEASE WAIT
ScreenChanged	1	No User	SYSTEM BUSY PLEASE WAIT
TruncateLog	3	No User	From: 2003-08-12 13:09:23.3 To: 2003-08-12 13:11:16.6
UserTokenPresent	1	Issuer: 4294967295 SerialNo: 100000004	
UserTokenInvalid	2	Issuer: 4294967295 SerialNo: 100000006	I&A Certificate Not Verifiable
DisplayChanged	1	No User	ENTRY DENIED / REMOVE TOKEN
ScreenChanged	1	No User	WELCOME TO TIS
UserTokenRemoved	2	Issuer: 4294967295 SerialNo: 100000006	
DisplayChanged	1	No User	WELCOME TO TIS / ENTER TOKEN

3.33.4.2 Keystore

keystore is unchanged.

3.33.4.3 Config data

Unchanged.

3.33.4.4 Visual

Screen Entity	**Status**
Door Alarm	OK throughout test
Audit Alarm	Failed throughout test
Configuration Data	Never displayed.
System Stats	Never displayed.
Messages	Values as detailed in audit log ScreenChanged entries.

4 Index of Tests

Document Control and References

Changes history

Issue 0.1 (4 September 2003): Initial draft for review.

Issue 1.0 (8 September 2003): Provisional issue following internal review. Two tests added following review.

Issue 1.1 (19 August 2008): Updated for public release.

Changes forecast

Incorporation of comments from NSA.

Document references

1 TIS Formal Design, S.P1229.50.1.