Tokeneer ID Station

Installation Guide and User Manual

S.P1229.73.1
Issue: 1.2
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 installation guide and user manual for the TIS (Tokeneer ID Station) software supplied by Praxis.

This document serves two purposes. It describes how to install the TIS application. It also describes how to use TIS once the application is installed.

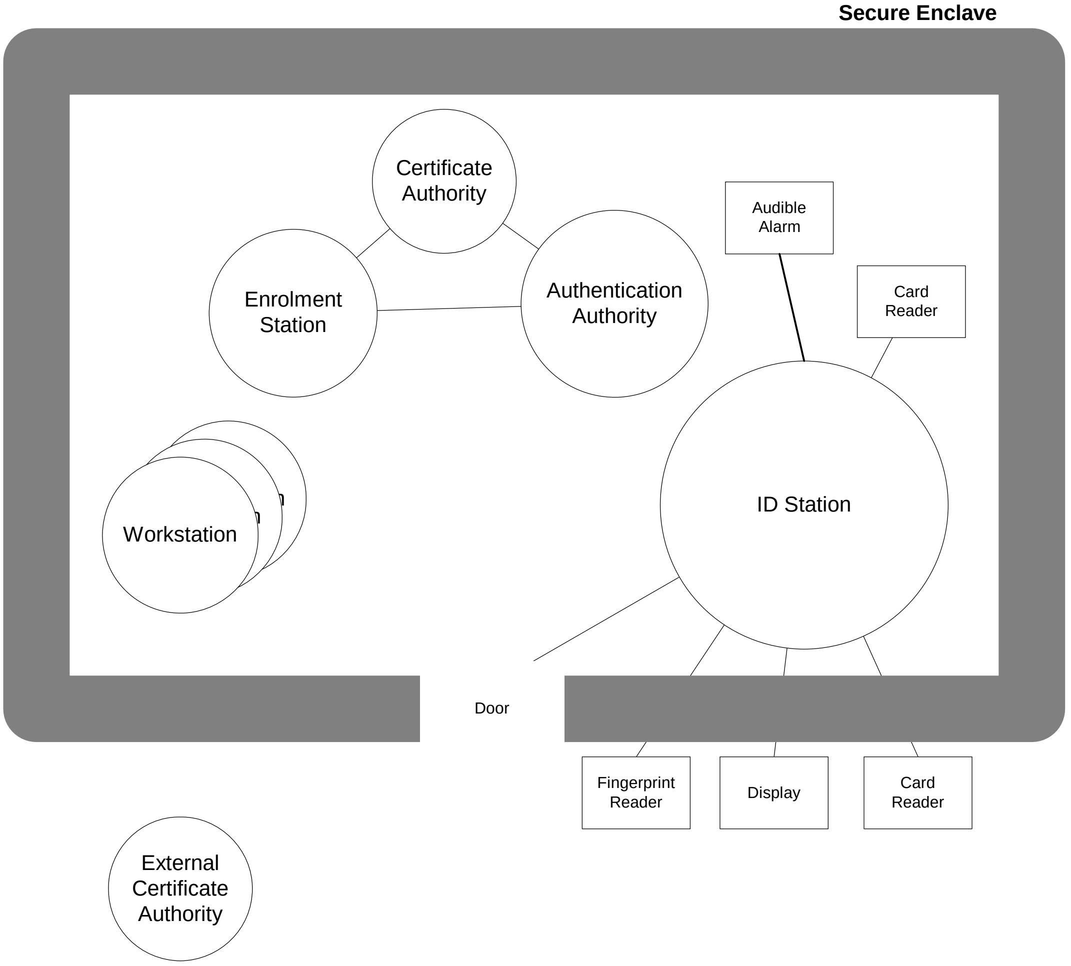
1.3 Scope

This application was produced to demonstrate a high-integrity development process. However the development process does not address the issues of attaining the necessary operating system security that would be required to ensure the application is protected from malicious attack. This was considered outside the scope of this project.

If this application were to be used in a secure environment, operating system constraints would need to be applied to prevent user access to the files used by the TIS application. The installation does not address any of these issues and as such the application is known to be vulnerable to attack through modification of configuration data, keystore data and the audit log.

1.4 Context

The TIS developed here is a single component in a larger system.



Overall Tokeneer System:

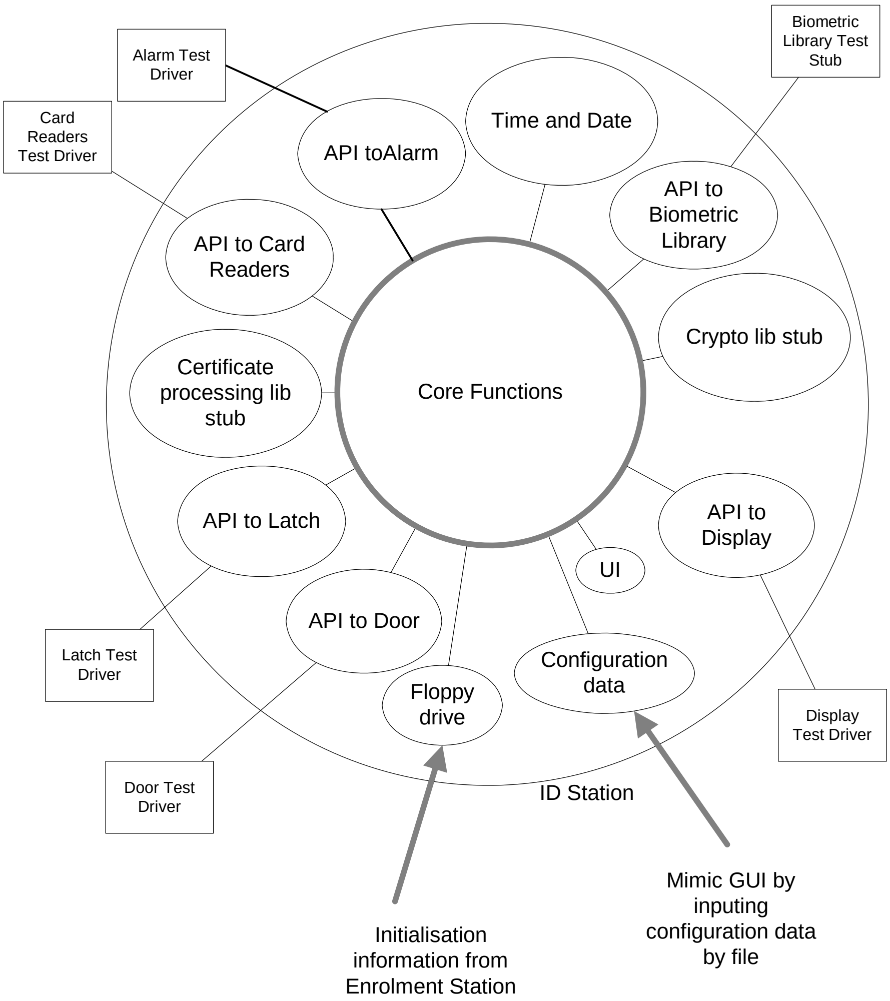
The complete Tokeneer system consists of a secure enclave and a set of system components, some housed inside the enclave and some outside.

The ID Station interfaces to five different physical devices:

Fingerprint reader
Smartcard reader (two instances)
Door
Audible Alarm
Visual display

These five interfaces are modelled by Test devices supplied by SPRE Inc on a separate machine.

There is a sixth interface via the floppy drive, used to take initialisation data from the Enrolment Station and to take configuration data in, and audit data out.



TIS structure

The peripherals are replaced by Test Drivers; the drivers by message translation mechanisms; and the libraries by stubs. The GUI is mimicked by a file, and simple command line interaction.

Praxis has developed the Core Functions according to their high-integrity development process, and the support functions using good engineering practice (but without the application of all the high integrity processes). The Core Functions combined with the support functions form the TIS application.

2 Installation guide

2.1 Required resources

2.1.1 Hardware

This TIS application should be executed on an IBM Compatible PC.

The machine on which TIS executes must have a Floppy Drive.

The TIS application requires at least 3Mb of memory to run and a further 6Mb of free disk space, which will be taken up by files created by the TIS application.

2.1.2 Software

The TIS application is a 32bit Windows application that will run on a Windows NT or Windows 2000 operating system.

The machine on which TIS executes must be configured for network access as the TIS application needs to communicate with the SPRE Test Devices.

The Floppy Drive should be configured as the first removable drive. This means that the Floppy Drive need not be the A: drive but if it is, for-instance, drive K:, then drives A to J must not be removable drives.

2.2 Installation process

Decide upon a directory in which to install TIS, eg C:\Program Files\TIS.

To install TIS, copy the executable **tis.exe** to the chosen location.

Add the location of the tis.exe to the System environment variable **path**.
A user with operating system administrator privileges can perform this from the Control Panel.

The TIS application can now be run from any location.

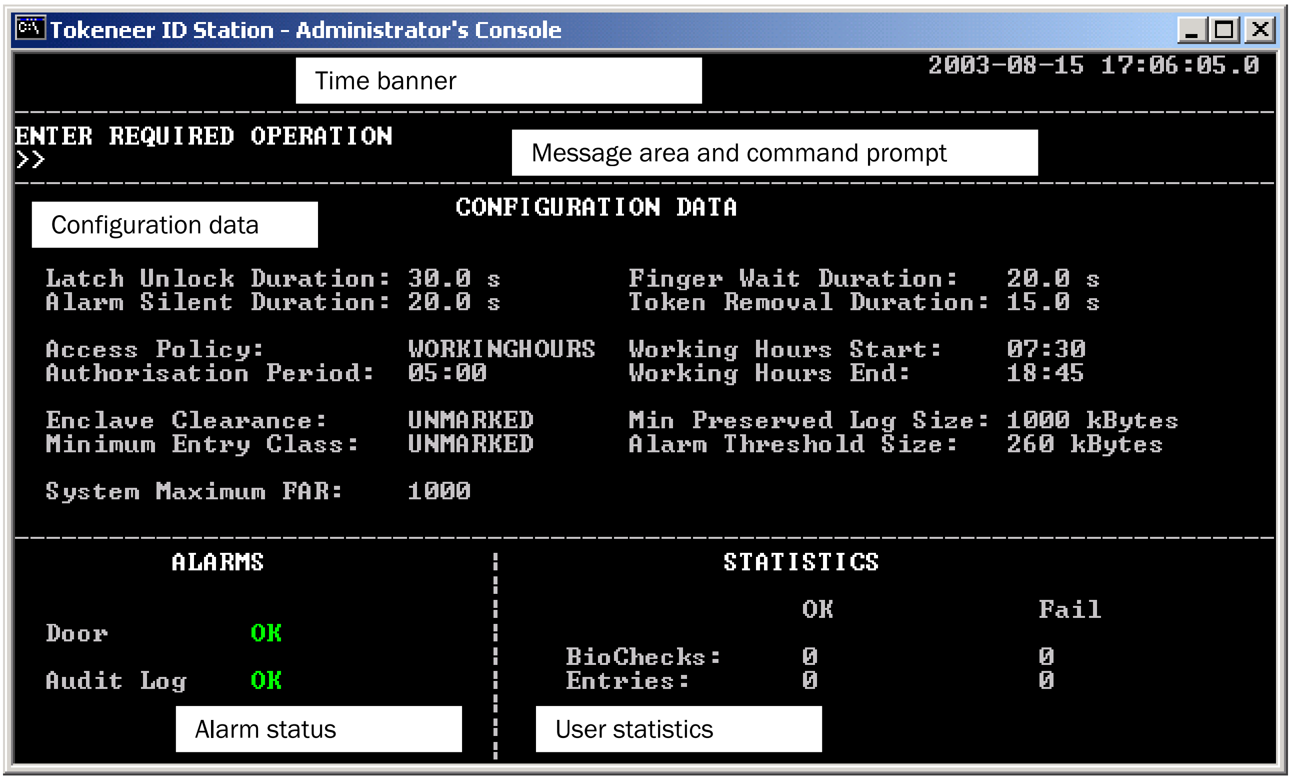
3 User Guide

This section of the document describes how to run the TIS application.

3.1 Summary of the User Interfaces to TIS

3.1.1 Administrator's Console

The Administrator's console window takes the format shown below. The screen is divided into 5 key components.



Tokeneer ID Station - Administrator's Console
Time banner
Message area and command prompt
Configuration data
Alarm status
User statistics

```
                                                     2003-08-15 17:06:05.0
--------------------------------------------------------------------------------
ENTER REQUIRED OPERATION
>>
--------------------------------------------------------------------------------
                              CONFIGURATION DATA

  Latch Unlock Duration: 30.0 s          Finger Wait Duration:   20.0 s
  Alarm Silent Duration: 20.0 s          Token Removal Duration: 15.0 s

  Access Policy:         WORKINGHOURS    Working Hours Start:    07:30
  Authorisation Period:  05:00           Working Hours End:      18:45

  Enclave Clearance:     UNMARKED        Min Preserved Log Size: 1000 kBytes
  Minimum Entry Class:   UNMARKED        Alarm Threshold Size:   260 kBytes

  System Maximum FAR:    1000
--------------------------------------------------------------------------------
          ALARMS                 :                 STATISTICS
                                 :
                                 :                      OK             Fail
  Door          OK               :
                                 :    BioChecks:        0              0
  Audit Log     OK               :    Entries:          0              0
                                 :
```

3.1.1.1 Time Banner

The time banner gives the current date and time. It is refreshed every time the system clock is polled.

The update frequency is highly dependent on the time taken to exchange messages between TIS and the Device Drivers.

3.1.1.2 Message area and Command Prompt

The message area gives a one-line message to the administrator.

The command prompt is on the line below the message and allows the administrator to type in the required operation when prompted to do so. The TIS ignores data typed into this area when commands are not prompted for.

3.1.1.3 Configuration data

Configuration data is only displayed when a security officer is present.

This panel on the console presents the current settings of the configuration data.

3.1.1.4 Alarm status

This panel on the console presents the current status of the door alarm and the audit log alarm. If the door alarm indicates FAIL then the door is not secure (or cannot be determined to be secure). Re-securing the enclave clears the door alarm. If the audit log alarm indicates FAIL then the audit log has exceeded the alarm threshold size or has been truncated. Archiving the audit log to bring the internally held log below the alarm threshold size clears the audit log alarm.

3.1.1.5 User statistics

This panel on the console presents the system statistics collected since the last time that the TIS was powered up. The statistics recorded capture the number of successful and failed entry attempts and the number of successful and failed biometric checks. A user entry attempt is considered successful if the system unlocks the door to allow an entry; there is no check to ensure that the door is subsequently opened.

3.1.2 Floppy Drive

The TIS accepts data during enrolment and when the system is re-configured from an external source. This data is provided on a floppy drive. In all cases the TIS application will prompt the user at the workstation for a floppy. TIS also exports archived log data to floppy. When a floppy is requested it either needs to contain data, in which case the data must be held in the sole file on the floppy, or it must contain no data, in which case it must be blank and formatted.

3.1.3 Other Peripherals

The remaining peripherals:

Door (at the portal)
Audible Alarm (at the workstation)
Smartcard reader (two instances, one outside the portal and one at the workstation)
Fingerprint Reader (outside the portal)
Visual Display (outside the portal)

are all modelled by test devices supplied by SPRE Inc. For information on how to interact with these test devices the reader is referred to [1].

Each of these test devices provides facilities to perform user interactions with the device. For example a user may “open”, “close”, or “breakOpen” the door.

3.2 Starting TIS

To start TIS, open a windows **command prompt**.

Change directory to the location at which you wish the application to run, and at which TIS will store its data.

Note TIS should always be started from the same location; this ensures that TIS starts up with the persistent state held when it was last shutdown.

From the command prompt type the following command:

- **tis** [<Test device server name> [<Workstation port> [<Portal #1 port>]]]

This command takes three optional arguments:

1. *Test device server name*, this is a text string giving the name of the server and must not exceed 30 characters. If no value is supplied the default value of **abqnm01.spre-inc.com** is used.

2. *Workstation port*, this is the number of the port supporting the devices on the TIS Kernel workstation. If no value is supplied the default value of **12000** is used.

3. *Portal #1 port*, this is the number of the port supporting the devices at Portal #1. If no value is supplied the default value of **12001** is used.

To supply any of the optional arguments, you must supply the preceding ones also.

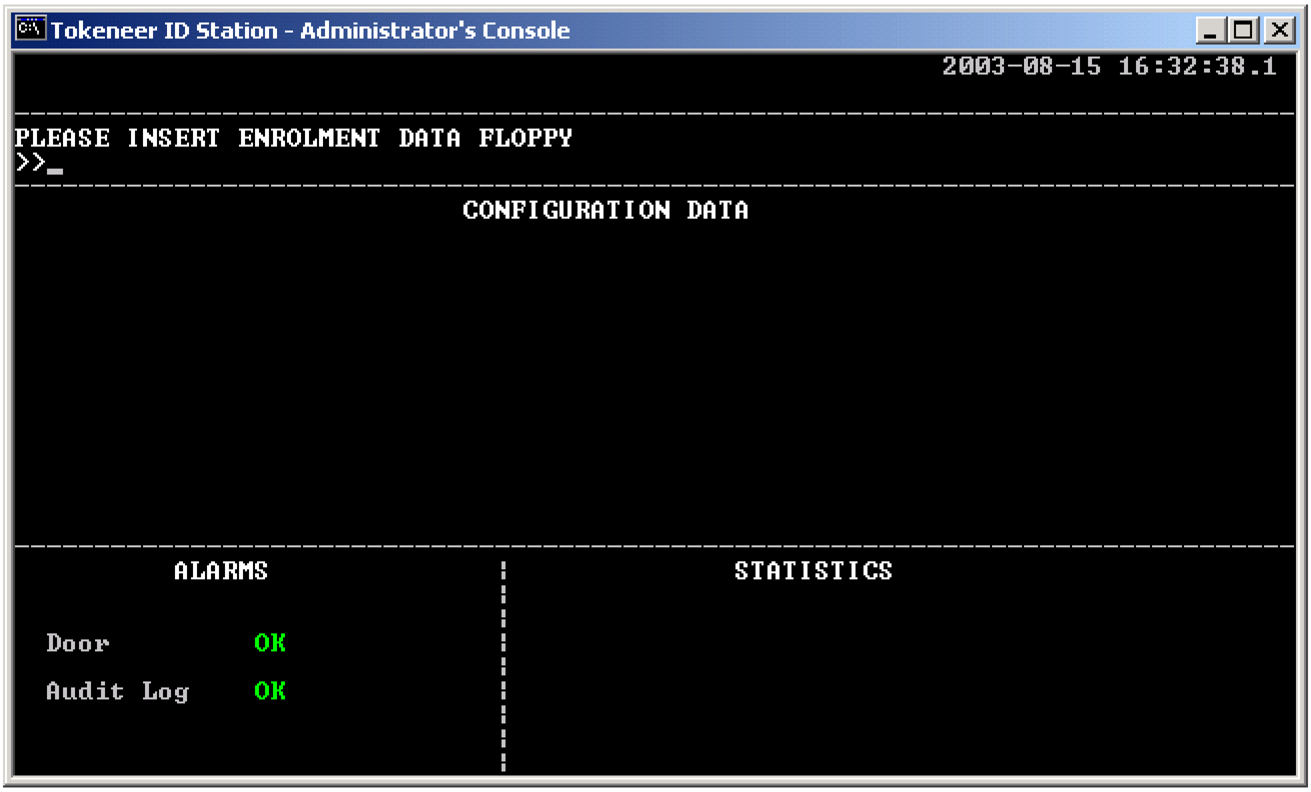
The following are example invocations of the TIS application.

- **tis abqnm02.spre-inc.com**
  Starts TIS using test device server abqnm02.spre-inc.com and ports 12000 and 12001.

- **tis**
  Starts TIS using the default arguments, test device server abqnm01.spre-inc.com and ports 12000 and 12001.

- **tis abqnm01.spre-inc.com 12000 12003**
  Starts TIS using test device server abqnm01.spre-inc.com and ports 12000 and 12003.

Depending on how large the current log file is, TIS may take over a minute to start-up. When it starts up successfully the following screen will be displayed.

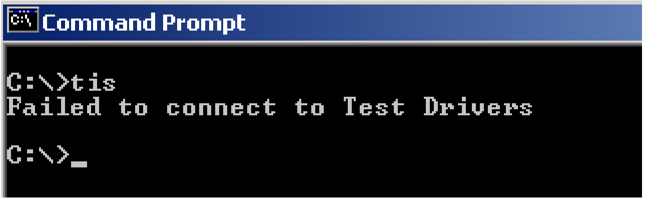


```
                                                        2003-08-15 16:32:38.1
--------------------------------------------------------------------------------
PLEASE INSERT ENROLMENT DATA FLOPPY
>>_
--------------------------------------------------------------------------------
                            CONFIGURATION DATA









--------------------------------------------------------------------------------
          ALARMS                  |              STATISTICS
                                  |
                                  |
  Door          OK                |
                                  |
  Audit Log     OK                |
                                  |
                                  |
```

Figure 1: TIS Administrator's console as displayed following the first start-up.

If a floppy is already present in the drive at start-up the message will not request a floppy.

If TIS is unable to connect to the test drivers then the application will terminate immediately and a message at the command prompt will indicate the failure to connect.



```
C:\>tis
Failed to connect to Test Drivers

C:\>_
```

Figure 2: TIS terminates when it cannot connect to the Test Drivers.

3.3 The initial system

When TIS is first started it creates three directories below the directory in which the application is invoked

.\System – This will be used to retain system information required by TIS through a power-down. It will contain the current **keystore** data and the current **configuration** data.

.\Log – This will be used by TIS to hold the audit log files.

.\Temp – This is used as a temporary file store by TIS. It is used to store files read and written to the floppy.

The user will have no need to access or modify any of the files in any of these directories. TIS will create the directories if they are not already present.

Subsequent invocations of TIS will make use of the information in the **.\System** and **.\Log** directory to define the initial state of the TIS.

For *test purposes* it is possible to un-enrol the TIS by deleting the contents of the .**System** directory, this will empty the keystore and result in the default configuration being used the next time that TIS is invoked. It should be noted that there is no requirement on TIS for un-enrolment or re-enrolment so no TIS functions have been provided to undertake these activities.

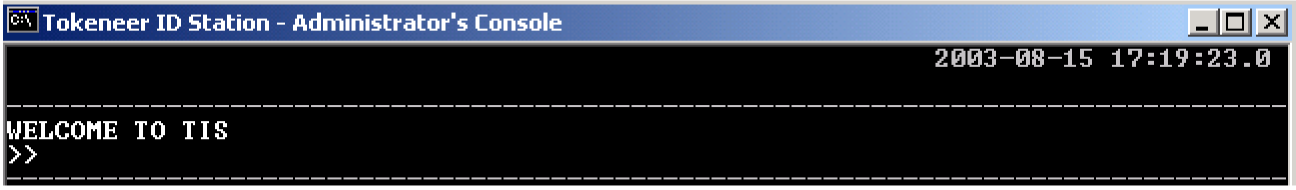
3.4 Enrolment

After initial start-up TIS will request the user for enrolment data (See Figure 1.)

Enrolment data takes the form of a number of ID certificates provided in a file on a floppy disk. There is no restriction on the name of the file although it must be the only file on the disk.

The exact format of enrolment data is given in Appendix A.

Following successful enrolment the Administrator's console message changes to a welcome message, as does the display at the enclave portal.



```
                                                        2003-08-15 17:19:23.0
--------------------------------------------------------------------------------
WELCOME TO TIS
>>
--------------------------------------------------------------------------------
```

Figure 3: Welcome Message displayed at the Administrator's Console

3.5 Administrative operations

There are four administrator operations that can be invoked from the Administrator's console. To perform an administrative operation an administrator must first log onto the TIS.

3.5.1 Logging On

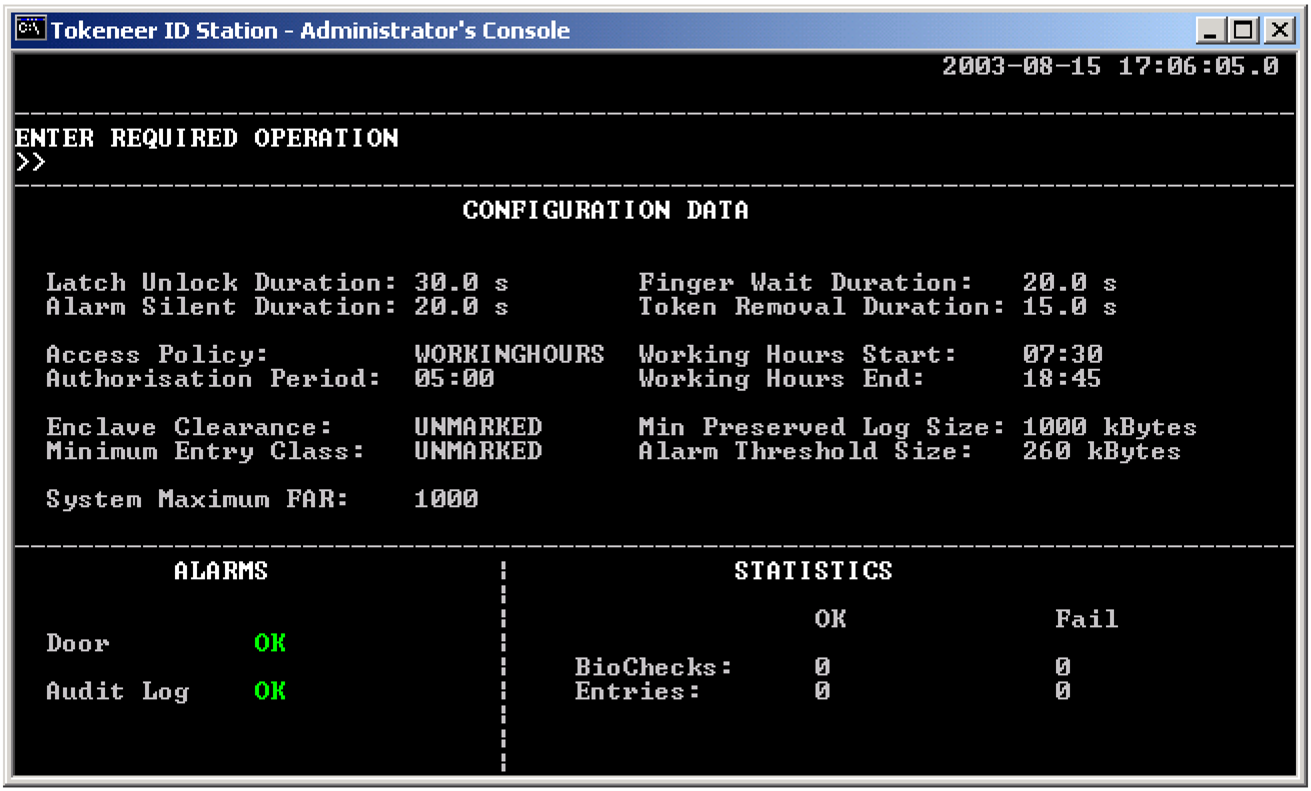
An administrator can log onto the TIS by inserting their card in the token reader at the TIS workstation.

The token will be accepted if it is valid and contains a current authorisation certificate (signed by the TIS) that gives the role of the user to be an administrative role.

The administrative roles are:

- Guard
- Security Officer
- Audit Manager

Once an administrator has logged on to the TIS workstation the administrator will be prompted to enter the operation they require. (See Figure 4)



Tokeneer ID Station - Administrator's Console

```
                                                                 2003-08-15 17:06:05.0
--------------------------------------------------------------------------------
ENTER REQUIRED OPERATION
>>
--------------------------------------------------------------------------------
                            CONFIGURATION DATA

  Latch Unlock Duration: 30.0 s          Finger Wait Duration:    20.0 s
  Alarm Silent Duration: 20.0 s          Token Removal Duration: 15.0 s

  Access Policy:         WORKINGHOURS    Working Hours Start:     07:30
  Authorisation Period:  05:00           Working Hours End:       18:45

  Enclave Clearance:     UNMARKED        Min Preserved Log Size: 1000 kBytes
  Minimum Entry Class:   UNMARKED        Alarm Threshold Size:    260 kBytes

  System Maximum FAR:    1000
--------------------------------------------------------------------------------
          ALARMS               |                STATISTICS
                               |
                               |                     OK            Fail
  Door          OK             |
                               |    BioChecks:      0              0
  Audit Log     OK             |    Entries:        0              0
                               |
```

Figure 4: TIS prompting the logged-on administrator for an operation.

Configuration data is only displayed when the Security Officer is logged-on.Statistics are displayed when any administrator is logged on.

The operations that can be performed by an administrator are presented in the sections below. An administrator with a given role only has authority to perform a subset of the available operations.

TIS is case-insensitive when accepting commands and where the command is long TIS will perform command completion as long as the first word of the command is present. So for example to update the configuration data we may type in any of the following commands:

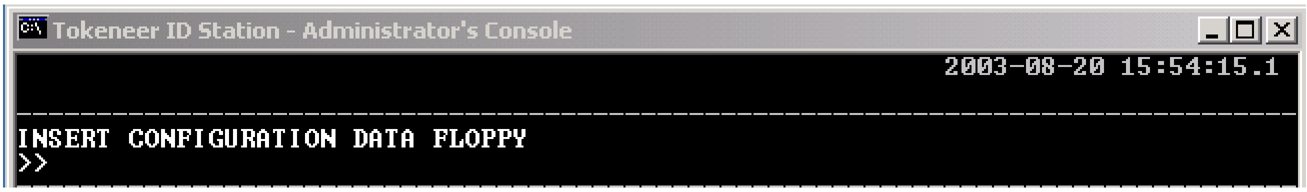
```
UPDATE CONFIG DATA
Update Config
UPDATE con
update
```

However “Update Data” is not valid as it cannot be extended to form the full command and “UP” is not valid as it is only part of the first word of the command.

3.5.2 Updating configuration data

Command	UPDATE CONFIG DATA
Shortest Command	UPDATE
Performed by	Security Officer

When updating the configuration data the security officer will need to supply configuration data on a floppy disk. If a floppy disk is not present in the drive the security officer is prompted to supply the configuration data. (See **Figure 5**)



```
                                                          2003-08-20 15:54:15.1
--------------------------------------------------------------------------------
INSERT CONFIGURATION DATA FLOPPY
>>
```

Figure 5: TIS request's the security officer to supply configuration data

The Floppy disk should contain exactly one file and this file must contain the new configuration data. The contents of the file must conform to the constraints presented in Appendix B.

If the supplied configuration data is invalid then the displayed configuration data will not change and the security officer will be warned that the data was invalid.

If the security officer removes their token before the operation has competed then the operation will fail.

If the supplied configuration data is valid then the displayed configuration data will be updated and the security officer will be prompted for another operation request.

3.5.3 Archiving the log

Command	ARCHIVE LOG
Shortest Command	ARCHIVE
Performed by	Audit Manager

When archiving the log the audit manager will be prompted to supply a blank floppy disk. TIS does not check that the floppy is blank but it cannot guarantee success if there are other files already present on the floppy.

The operation transfers the archived component of the log to floppy as a file named **archive.log**. If there is already a file by this name on the floppy disk it will not be overwritten and the archive will fail.

The archive will fail if the floppy disk is removed before the system has had time to check that the data written to floppy matches the data that the system attempted to archive.

If there are insufficient entries in the log to perform an archive (< 1024) then the archived file will be empty. This is not considered to be an error by TIS.

If the archive failed then the audit log will not be reduced in size and the audit manager will be warned that the archive failed.

If the audit manager removes their card before the operation is complete then the operation will fail.

Following a successful archive the audit log will be reduced in size by the number of entries that were written to the archive. If the audit alarm was alarming then this will be silenced if the audit activity removed sufficient entries to reduce the audit log to below the alarm threshold size. It may however be necessary to perform several archive operations to silence the audit alarm if the audit log has been allowed to grow for some time after the audit alarm was first raised. Following a successful archive the audit manager is prompted to perform another operation.

The format of the archived log file is presented in Appendix C. It presents information in fixed width, comma separated columns in a format that can be imported into spreadsheet programmes (such as Microsoft Excel) for analysis.

3.5.4 Shutdown

Command	SHUTDOWN
Shortest Command	SHUTDOWN
Performed by	Security Officer

The shutdown operation leaves the enclave door in a secure state and then terminates the TIS application.

If the door is currently open the security officer will be prompted to close the door as the door must be shut before the operation can complete.

The security officer may remove their token before the operation is complete, this will not prevent the operation from completing.

3.5.5 Overriding the door latch

Command	OVERRIDE LOCK
Shortest Command	OVERRIDE
Performed by	Guard

This operation releases the lock on the enclave door allowing a person to enter the enclave under the supervision of the guard.

If the guard removes their token before the lock has been released then the operation will fail.

Once the lock has been released the Enclave Display will indicate that entry is permitted and the guard will be prompted to perform a new operation.

3.5.6 Logging Off

To log off the administrator simply needs to remove their card from the token reader at the workstation.

This can be performed at any time but removing the administrators token during an operation will cause the operation to fail, except during a shutdown.

The Administrator will also be automatically logged off if the authorisation certificate on the token expires. This will only happen when the administrator is not performing an operation, allowing any operation that is in progress to be completed before the administrator is automatically logged off.

3.6 User Entry

In order for a user to enter the enclave and make use of the workstations held within the enclave the user must be authenticated by a two phase authentication process performed at a portal to the enclave controlled by TIS.

The user entry process is as follows (text in *italics* indicates actions required by the user, text in **bold** indicates a message presented to the user by TIS at the portal display):

1 TIS prompts a user to enter their token
WELCOME TO TIS / ENTER TOKEN

2 *The user supplies a valid token to the card reader at the portal.*
TIS will validate this token during which the following message is displayed:
AUTHENTICATING USER / PLEASE WAIT

3 If the token is valid but does not contain a current authorisation certificate TIS will need to perform biometric validation and will prompt the user to insert their finger into the finger-print reader:
AUTHENTICATING USER / INSERT FINGER

4 *The user inserts their finger into the fingerprint reader providing a biometric sample.*
The user must provide the fingerprint data within the configured time.
TIS will validate the fingerprint against information held on the token during which the following message is displayed:
AUTHENTICATING USER / PLEASE WAIT

5 TIS writes an authorisation certificate and determines whether the user has appropriate clearance to enter the enclave.

6 If the user has a sufficiently high clearance then the user is prompted to remove their token and enter the enclave.
REMOVE TOKEN AND ENTER

7 *The user must remove their token to unlock the door.*
The user must remove their token within the configured time. Once the token has been removed TIS will unlock the enclave door and prompt the user to enter:
ENTER ENCLAVE

8 *The user enters the enclave.*

9 Once the door has been unlocked for the configured duration TIS will relock the door and prompt a new user to enter their token and start the validation process.

If at any point during the validation process a failure occurs, either due to data being invalid, or the user having insufficient clearance, or the user failing to respond within the allotted time, the user will be prompted to remove their token with the message **ENTRY DENIED / REMOVE TOKEN**.

If the user already has a valid authorisation certificate on their token then biometric verification will not be requested and the entry procedure will jump from step 2 to step 6, omitting steps 3-5.

If the user removes their token before requested to do so by TIS then the user entry is aborted and TIS prompts a new user to enter their token.

A Appendix: Enrolment Data Format

Enrolment data is supplied as a number of ID certificates within a single file. Each ID Certificate takes the same format as a certificate transmitted across the TCP/IP interface to the device drivers (although the outermost braces enclosing the certificate “dictionary” are omitted). Each certificate will appear as a string on a single line within the enrolment data file.

The first ID certificate in the file must be that of the CA that issued the TIS ID Certificate, the second ID certificate in the file must be the ID certificate of the TIS being enrolled. The remaining certificates may be in any order as long as the ID certificate of a CA precedes any ID certificates issued by that CA.

The format of the certificate is as presented in Table 1, non-bold text appears in the file as presented here, bold text is defined in the subsequent table. Return characters should not appear in the string, they are used here to improve layout, similarly space characters are optional and will be ignored within the processing.

ID Certificate format within Enrolment file

```
'CertLength': 'CertificateLength',
'CertDataT':
        {'CertType': '0',
        'SerialNumber': 'SerialNumber',
        'SigAlgID': 'Algorithm',
         'Issuer': {'Text': 'IssuerText',
                   'ID': 'IssuerID',
                   'TextLength': 'IssuerTextLength'},
        'Validity': {'NotAfter': {'Minute': 'Minute',
                                 'Month': 'Month',
                                 'Day': 'Day',
                                 'Hour': 'Hour',
                                 'Year': 'Year'},
                    'NotBefore': {'Minute': 'Minute',
                                 'Month': 'Month',
                                 'Day': 'Day',
                                 'Hour': 'Hour',
                                 'Year': 'Year'}},
        'Subject': {'Text': 'UserText',
                   'ID': 'UserID',
                   'TextLength': 'UserTextLength'},
        'SubjectPublicKeyInfo': {'KeyLength': 'KeyLength',
                                'AlgoRithmID': 'Algorithm',
                                'KeyID': 'KeyID'},
        'CryptoControlData': {'DigestFinalReturn': 'ReturnValue',
                             'DigestLength': 'DigestLength',
                             'DigestUpdateReturn': 'ReturnValue',
                             'Digest': {'VerifyReturn': 'ReturnValue',
                                       'SignReturn': 'ReturnValue',
                                       'DigestID': 'DigestID'}},
        'SignatureData': {'AlgoRithmID': 'Algorithm',
                         'SigLength' : 'SigLength',
                         'Signature': {'KeyID': 'KeyID',
                                      'DigestID': 'DigestID'}}}
```

Table 1 ID certificate structure within enrolment file

Values taken by entities in bold are presented in Table 2. Constraints on valid ID certificates are detailed in Table 3.

Certificate Entity	valid values
Algorithm	string with the following values: RSA MD2 MD5 SHA_1 RIPEMD128 RIPEMD160 MD2_RSA MD5_RSA SHA1_RSA RIPEMD128_RSA RIPEMD160_RSA
CertificateLength	numeric string range 0 .. 4050
Day	numeric string range 01 .. 31
DigestID	numeric string range 0 .. 2^{32} -1
DigestLength	numeric string range 0 .. 32
Hour	numeric string range 00 .. 23
IssuerTextLength	numeric string range 0 .. 40
IssuerId	numeric string range 0 .. 2^{32} –1
IssuerText	ASCII string with maximum length of 40 characters (no CR or LF characters).
KeyID	numeric string range 0 .. 2^{32} -1
KeyLength	numeric string range 0 .. 128
Minute	numeric string range 00 .. 59
Month	numeric string range 01 .. 12
ReturnValue	string with one of the following values OK HostMemory GeneralError FunctionFailed ArgumentsBad AttributeReadOnly AttributeTypeInvalid AttributeValueInvalid DataInvalid DataLenRange DeviceError DeviceMemory FunctionCanceled KeyHandleInvalid KeySizeRange KeyTypeInconsistent KeyFunctionNotPermitted MechanismInvalid MechanismParamInvalid ObjectHandleInvalid OperationActive OperationNotInitialized SignatureInvalid SignatureLenRange TemplateIncomplete TemplateInconsistent BufferTooSmall CryptokiNotInitialized CryptokiAlreadyInitialized
SerialNumber	numeric string range 0 .. 2^{32} -1
SigLength	numeric string range 0 .. 128
UserId	numeric string range 0 .. 2^{32} –1
UserText	ASCII string with maximum length of 40 characters
UserTextLength	numeric string range 0 .. 40
Year	numeric string range 1901 .. 2099

Table 2 Valid values of fields

Constraint	**Description**
Date exists	Both the **NotBefore** and **NotAfter** dates must be real dates. Setting Month to 2 and Day to 30 would always be invalid
Certificate length correct	The certificate length is the number of characters in the string starting from the '**{**' following **CertDataT** field to the final '**}**'.
Algorithm consistent	The **SignatureData.AlgorithmID** and **SigAlgID** must match, this algorithm must also be a combined algorithm including an encryption mechanism and a digest mechanism (i.e. one of MD2_RSA, MD5_RSA, SHA1_RSA, RIPEMD128_RSA or RIPEMD160_RSA).
Signature not too long	The **SigLength** field must be no larger than the length of the key used to sign the certificate.
Returns OK	The crypto control data detailing the return values crypto operations **DigestUpdateReturn**, **DigestFinalReturn** and **VerifyReturn** must be set to OK. This indicates that these functions will succeed.
Digest matches signed digest	The **SignatureData.Signature.DigestID** must match **CryptoControlData.Digest.DigestID**. This represents the digest used to create the signature being the same as the digest calculated from the raw certificate data.
signing key matches issuer	The **SignatureData.Signature.KeyID** must match the key id associated with the **Issuer.ID**. This will be the **KeyID** supplied within the **SubjectPublicKeyInfo** of the Issuer's ID certificate.

Table 3 Constraints on valid certificates

B Appendix: Configuration Data Format

The format of a configuration data file is presented in the next table. Each field is presented on a new line and takes the form of a field identifier followed by one space and the value of the field. Each line is terminated by a CR and LF. There should be no spaces between the end of the field value and the end of the line.

The file formats have been selected to provide a user-friendly interface for entering values. This includes restricting the granularity of short timeout durations to 1 second, the granularity of longer times to minutes and the granularity of file sizes to kBytes.

File format	comments
ALARMSILENTDURATION nnn	value is in seconds range 00..200
LATCHUNLOCKDURATION nnn	value is in seconds range 00..200
TOKENREMOVALDURATION nnn	value is in seconds range 00..200
FINGERWAITDURATION nnn	value is in seconds range 00..200
ENCLAVECLEARANCE tttttt	values of “ttttt” are unmarked, unclassified, restricted, confidential, secret, topsecret
WORKINGHOURSSTART hh:mm	00:00 represents midnight, max value is 23:59
WORKINGHOURSEND hh:mm	00:00 represents midnight, max value is 23:59
MAXAUTHDURATION hh:mm	max value is 10:00
ACCESSPOLICY tttttt	values of “tttttt” are allhours and workinghours
MINENTRYCLASS ttttt	values of “ttttt” are unmarked, unclassified, restricted, confidential, secret, topsecret *This field must have no higher classification than the value given for ENCLAVECLEARANCE*.
MINPRESERVEDLOGSIZE nnnn	value is in kBytes range 0 .. 4096
ALARMTHRESHOLDSIZE nnnn	value is in kBytes range 0 .. 4096 *This field must be no greater than the value given for MINPRESERVEDLOGSIZE.*
SYSTEMMAXFAR nnnnnnnnnn	INTEGER32 value nnnnnnnnnn/(2^{31} – 1) is the required probability of false acceptance.

An example configuration data file is given in Figure 6.

```
ALARMSILENTDURATION 20
LATCHUNLOCKDURATION 30
TOKENREMOVALDURATION 15
FINGERWAITDURATION 20
ENCLAVECLEARANCE unmarked
WORKINGHOURSSTART 07:30
WORKINGHOURSEND 18:45
MAXAUTHDURATION 05:00
ACCESSPOLICY workinghours
MINENTRYCLASS unmarked
MINPRESERVEDLOGSIZE 1000
ALARMTHRESHOLDSIZE 260
SYSTEMMAXFAR 1000
```

Figure 6: An example configuration file

C Appendix: Audit Log Archive Format

Audit log data is exported during an archive.

The audit file contains a number of audit entries with the following properties.

- each audit entry is terminated by a CR (Carriage return) and LF (Line feed). The entry itself does not contain any LF or CR.
- each field of an audit entry is comma separated and has a fixed width. Individual fields do not contain commas.

The fields of an audit entry are presented it the order and format given in the table below:

field	format	comments
time	yyyy-mm-dd hh:mm:ss.s	Time is displayed to 1/10th second accuracy. The field is 21 characters.
severity	n	Allowed values "1" – info; "2" – warning, "3" – critical. This field is 2 characters.
id	nn	Numeric index of the audit element type. see Table 4. *For example StartUnenrolledTIS has value 0.* This field is 3 characters.
type	ASCII text	Text name for the given audit element type see Table 4. This field is 20 characters.
user	ASCII text	Text description identifying user in the form "Issuer: xxx SerialNo: yyy" or "NoUser". Where the user can be identified the identity is taken from the ID Certificate using the Issuer.ID and SerialNumber fields. This field is 50 characters.
description	ASCII text	free text description containing additional information This field is 150 characters.

Where "n" represents a single ASCII digit.

Audit element	Index
STARTUNENROLLEDTIS	0
STARTENROLLEDTIS	1
ENROLMENTCOMPLETE	2
ENROLMENTFAILED	3
DISPLAYCHANGED	4
SCREENCHANGED	5
DOORCLOSED	6
DOOROPENED	7
LATCHLOCKED	8
LATCHUNLOCKED	9
ALARMRAISED	10
ALARMSILENCED	11
TRUNCATELOG	12
AUDITALARMRAISED	13
AUDITALARMSILENCED	14
USERTOKENREMOVED	15
USERTOKENPRESENT	16
USERTOKENINVALID	17
AUTHCERTVALID	18
AUTHCERTINVALID	19
FINGERDETECTED	20
FINGERTIMEOUT	21
FINGERMATCHED	22
FINGERNOTMATCHED	23
AUTHCERTWRITTEN	24
AUTHCERTWRITEFAILED	25
ENTRYPERMITTED	26
ENTRYTIMEOUT	27
ENTRYDENIED	28
ADMINTOKENPRESENT	29
ADMINTOKENVALID	30
ADMINTOKENINVALID	31
ADMINTOKENEXPIRED	32
ADMINTOKENREMOVED	33
INVALIDOPREQUEST	34
OPERATIONSTART	35
ARCHIVELOG	36
ARCHIVECOMPLETE	37
ARCHIVECHECKFAILED	38
UPDATEDCONFIGDATA	39
INVALIDCONFIGDATA	40
SHUTDOWN	41
OVERRIDELOCK	42
SYSTEMFAULT	43

Table 4 Audit element values

An example fragment of an audit log is presented in Figure 7.

```
2003-08-20 15:50:03.7, 1,  1, STARTENROLLEDTIS    , NoUser                                            ,
2003-08-20 15:50:39.7, 1, 29, ADMINTOKENPRESENT   , Issuer:  4294967295 SerialNo:   100000001         ,
2003-08-20 15:50:39.7, 1, 30, ADMINTOKENVALID     , Issuer:  4294967295 SerialNo:   100000001         ,
2003-08-20 15:50:39.7, 1,  5, SCREENCHANGED       , NoUser                                            , ENTER REQUIRED OPERATION
2003-08-20 15:50:57.8, 1,  5, SCREENCHANGED       , NoUser                                            , PERFORMING OPERATION PLEASE WAIT
2003-08-20 15:50:57.8, 1, 35, OPERATIONSTART      , Issuer:  4294967295 SerialNo:   100000001         , UPDATE CONFIG
2003-08-20 15:51:03.9, 1,  5, SCREENCHANGED       , NoUser                                            , INSERT CONFIGURATION DATA FLOPPY
2003-08-20 15:55:05.8, 1,  5, SCREENCHANGED       , NoUser                                            , PERFORMING OPERATION PLEASE WAIT
2003-08-20 15:55:11.0, 2, 40, INVALIDCONFIGDATA   , Issuer:  4294967295 SerialNo:   100000001         ,
2003-08-20 15:55:11.0, 1,  5, SCREENCHANGED       , NoUser                                            , INVALID DATA: PLEASE ENTER NEW OPERATION
```

Figure 7: Extract from an audit log

Document Control and References

Praxis High Integrity Systems Limited, 20 Manvers Street, Bath BA1 1PX, UK.

This material was originally developed by Praxis High Integrity Systems Ltd. under contract to the National Security Agency.

Changes history

Issue 0.1 (21 August 2003): Initial issue for internal review.

Issue 1.0 (22 August 2003): Provisional Issue following internal review.

Issue 1.1 (10 September 2003): Update to incorporate correction to fault S.P1229.6.53

- Clarify that administrator privileges are required to update the path system variable.
- Clarify that the system only requests a floppy if it is not present when required.
- Indicate how the system can be un-enrolled for test purposes.

Issue 1.2 (19 August 2008): Updated for public release.

Changes forecast

Updates following NSA review comments.

Document references

1 TIS Device Drivers ver 0.3, SPRE Inc Document D0409-01v03TIS Device Drivers.sxw, 12 June 2003.