Tokeneer ID Station
Annotated Summary of Security Target Exclusions

S.P1229.40.3
Issue: 1.0
Status: Definitive
19th August 2008

Originator

David Cooper

Approver

Janet Barnes (Project Manager)

Copies to:

National Security Agency

Praxis High Integrity Systems
File

SPRE Inc.

Contents

1 Introduction **3**
1.1 Background 3
1.2 Mark-up 3

2 TOE Description **4**
2.1 Organisational Security Policies 5

3 Security Objectives **6**
3.1 Security Objectives for the TOE 6

4 IT Security Requirements **8**
4.1 TOE Security Requirements 8

Document Control and References **11**
Changes history 11
Changes forecast 11
Document references 11

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 re-develop part of an existing secure system (the Tokeneer System) in accordance with their own high-integrity development process. This re-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.

This security target is a specialisation of the Protection Profile given in [1], and *should not be read in isolation*.

1.2 Mark-up

This marked up summary of the PP exclusions identifies the reasons why each exclusion has been made. No rationale is supplied for those aspects of the PP that are *included*; everything that can reasonably be done that is asked for in the PP will be included unless there is a reason for excluding.

In each case, a clause from the PP has been excluded primarily due to budget restrictions. With a larger budget all the functionality described in the PP could be implemented (with our current level of understanding of the functionality). But in addition to the budget constraints, this document highlights the secondary rationale for exclusion, one of:

CC:	our approach to the common criteria, focussing on functional security properties and those mechanisms that are demanded to achieve the functional security in the face of identified threats in a defined environment, would not require this clause.
core:	the function or area is beyond the scope of core functions discussed in the start-up meeting.
SPARK:	the development strategy of using formal methods (Z) and flow-analysed code (SPARK) prevents this clause from being implemented.

Only the lists of exclusions are included in the document — all other parts of the security target have been deleted.

2 TOE Description

The TOE matches the TOE described in [1], except as follows:

CC	core	SPARK		
	X		The TOE controls only the entry to the secure enclave, not the egress. There is no exit station, and no exit functionality.	No exit functionality was discussed at the start-up meeting.
	X		No keypad is provided — only two-factor authentication is supported.	Three-factor authentication was discussed at the start-up meeting and agreed out of scope.
	X		The Voice box does not form part of the TOE.	
	X		The TOE manages a single portal, not multiple portals.	The functionality discussed at the start-up meeting dealt with only a single portal.
	X		No certificate revocation lists (CRLs) are supported.	CRLs were explicitly agreed out of scope at the start-up meeting.
X			Communications between peripherals and the central unit of the TOE are assumed protected by other means, and no technical secure communications is provided.	Suitable choice of benign environment allows technical protection unnecessary.
X			No replay protection on the biometric device is supported.	Suitable choice of a benign environment allows technical protection to be unnecessary.
X	X		Internal integrity checks, manual integrity checks, diagnostics and decommissioning are not supported.	Suitable choice of a benign environment allows technical protection to be unnecessary. Decommissioning was not discussed in the start-up meeting, and has been excluded.
X			No backup or restore is supported.	The amount of information to be backed up is not sufficient for this to be a necessary security feature.

Details of the these exclusions are given in the relevant sections later in this Security Target.

2.1 Organisational Security Policies

The statements of section 3.3 of [1] apply except:

CC	core	SPARK		
	X		DP.Audit_Protect	Accounting (writing audit records) is in scope, but the protection of access to audit records, and their analysis is out of scope of the core TIS.
X			P.Availability	With suitable manual fall-back procedures we can prevent the environment from *needing* TIS to be running, and hence can make automated access low-availability.
X	X		DP.Screen_Locking	No GUI is being developed, and no requirements on the GUI are in scope. Given the simplicity of the Admin access, procedures can be defined that require Administrators to logon (by inserting their token), perform their actions, then log-off (by removing their token), without ever leaving the ID Station unattended. If they need to leave, they log off.
X			DP.Integrity	The TOE is not subject to any special threat of corruption (radiation, heat, physical attack, etc.) and so the monitoring of system integrity is not necessary. If more detailed security analysis were carried out, it may suggest specific areas that need to be protected (e.g. crypto keys in memory, or configuration data stored between power-up), in which case we would wish to identify focused security requirements for these areas.
X			P.Marking	The only outputs are the audit logs. Protection of protectively marked material is not a prime requirement for TIS, and I would encourage its exclusion from evaluation.
X			P.Physical_Control	The TOE is not subject to any special threat of corruption (radiation, heat, physical attack, etc.) and so physical protection is out of scope of this redevelopment project.

3 Security Objectives

3.1 Security Objectives for the TOE

In addition, the statements of section 4.1 of [1] apply except:

CC	core	SPARK		
	X		O.Audit_Account	No audit analysis or presentation functionality is supported. Audit archiving is the only facility to allow audit to be inspected.
	X		O.Code_Signing	There is no downloaded code. Installation is manual and not covered by technical security.
	X		O.Crypto_Data_Sep	Due to the simulation of the cryptographic module, this cannot be guaranteed.
	X		O.Crypto_Import_Export	Due to the simulation of the cryptographic module, this cannot be guaranteed.
	X		O.Crypto_Key_Man	Due to the simulation of the cryptographic module, this cannot be guaranteed.
	X		O.Crypto_Self_Test	Due to the simulation of the cryptographic module, this is not in scope of this redevelopment project.
	X		O.External_Labels	No data is exported to external systems, apart from the information written to the Token.
X			O.Fault_Tolerance	The TOE is not subject to any special threat of corruption (radiation, heat, physical attack, etc.) and so fault tolerance is not a security requirement. If more detailed security analysis were carried out, it may suggest specific functions that may need fault tolerance (e.g. audit archive), in which case we would wish to identify focused security requirements for these functions.
X			O.General_Integ_Checks	See DP.Integrity
X			O.I&A_Transaction	Audit will record actions at a sufficient level of detail.
X			O.Identify_Unusual_Act	The assumptions about the benign environment suggest that such measures would be unnecessary.
X			O.Info_Flow_Control	There are no security issues to do with information flow.
X			O.Integ_Sys_Dat_Int	See DP.Integrity
X			O.Integrity_Data/SW	See DP.Integrity
X			O.Integrity_Data_Rep	See DP.Integrity
X			O.Integrity_Practice	See DP.Integrity

CC	core	SPARK		
			O.Screen_Lock	No GUI is being developed, and no requirements on the GUI are in scope. Given the simplicity of the Admin access, procedures can be defined that require Administrators to logon (by inserting their token), perform their actions, then log-off (by removing their token), without ever leaving the ID Station unattended. If they need to leave, they log off.
X			O.Storage_Integrity	See DP.Integrity
	X		O.Sys_Access_Banners	No GUI is being developed, and no requirements on the GUI are in scope.
X			O.Sys_Backup_Procs	Backup and restore is not within scope for this redevelopment project. The amount of information that would be backed up is not sufficient to drive this as a security consideration
X			O.Sys_Backup_Restore	See O.Sys_Backup_Restore
X			O.Sys_Backup_Storage	See O.Sys_Backup_Restore
X			O.Sys_Backup_Verify	See O.Sys_Backup_Restore
X			O.Sys_Self_Protection	See DP.Integrity
X			O.Tamper_ID	See DP.Integrity
X			O.Trusted_DS_Recover	See DP.Integrity
X			O.Trusted_Recovery	See DP.Integrity
X			O.Trusted_Recovery_Doc	See DP.Integrity
X			O.User_Data_Integrity	See DP.Integrity

4 IT Security Requirements

4.1 TOE Security Requirements

4.1.1 TOE Security Functional Requirements

The statements of section 5.1 (and all its subsections) of [1] apply except:

CC	core	SPARK		
	X		Access Control Table (Table 3): Delete rows on Audit Configuration, Audit data, Revocation lists, and Backup data. Delete all "View" functions. Delete Craft Person. Add the ability of the Auditor to export audit data.	These changes are due to exclusions of other functionality, such as audit analysis. System maintenance, upgrade, etc. is beyond the primary scope.
	X		SFP.Digital_Signing	Cryptography will be simulated
X	X		In FAU_GEN.1, delete the following auditable events: FAU_SAR.1 FAU_SAR.2 FAU_SAR.3 FCO_NRO.2 FPT_AMT.1 FPT_ITT.3 FPT_RCV.2 FPT_RCV.4 FPT_RPL.1 FPT_TRC.1 FPT_TST.1 FTA_SSL.1 FTA_SSL.2	these are all deleted due to the non-support of the associated functions
	X		FAU_SAR.1	The Auditor will be able to export the audit archive, but all viewing and analysis functions will be done externally.
	X		FAU_SAR.2	The Auditor will be able to export the audit archive, but all viewing and analysis functions will be done externally.

	X		FAU_SAR.3	The Auditor will be able to export the audit archive, but all viewing and analysis functions will be done externally.
X			FAU_STG.2	See DP.Integrity
	X		FCS_CKM.1	No cryptographic key generation is being performed.
	X		FCS_CKM.2	No cryptographic key generation is being performed.
	X		FCS_CKM.4	No cryptographic key destruction is being performed.
	X		FDP_ETC.2	No secure data is being exported.
X			FPD_IFC.2	There are no security issues to do with information flow.
X			FDP_IFF.2	There are no security issues to do with information flow.
X			FDP_ITC.1	No user data is being imported.
X			FDP_ITC.2	No user data is being imported.
X			FDP_SDI.1	See DP.Integrity
	x		FMT_REV.1	No revocation is supported.
	X		FMT_SMR.2.3	Decommissioning is not supported.
X			FPT_AMT.1	See DP.Integrity
X			FPT_ITT.2	See DP.Integrity
X			FPT_ITT.3	See DP.Integrity
X			FPT_PHP.3	The TOE is in a secure area, and no protection against physical attack is required.
X			FPT_RCV.2	See DP.Integrity
X			FPT_RCV.4	See DP.Integrity
X			FPT_RPL.1	Replay protection is not within scope of this redevelopment project.
X			FPT_SEP.1	The TOE is being developed on a standard operating system. Any such protection will need to be supplied by the operating system.
X			FPT_TRC.1	See DP.Integrity
X			FPT_TST.1	See DP.Integrity
X			FRU_FLT.2	See DP.Integrity
	X		FTA_SSL.1	No GUI is being developed, and no requirements on the GUI are in scope.
	X		FTA_SSL.2	No GUI is being developed, and no requirements on the GUI are in scope.
	X		FTA_TAB.1	No GUI is being developed, and no requirements on the GUI are in scope.
	X		FTA_TSE.1	No revocation lists are supported.

CC	core	SPARK		
	X		Section 5.1.7, table. Only configuration data will be modifiable, and then only by the security officer. No restrictions will be imposed on the changes that can be made. Any necessary controls are out of scope of this redevelopment project	.
	X		Under FMT_MTD.1.1, use modified table 3 instead	

4.1.2 TOE Security Assurance Requirements

The statements of section 5.2 of [1] apply except:

In 5.2.6:

CC	core	SPARK		
		X	"tests" will be taken to include SPARK analysis	This should be regarded as an alternative, and more powerful, interpretation of the word "test". It will require accreditor buy-in.

5.2.7:

CC	core	SPARK		
X			AVA_CCA.1	Covert channels are not a security issue for this TOE.
	X		AVA_VLA.3	Vulnerability analysis will not be carried out, although it would usually be expected to be done for this TOE. It has been put out of scope for this redevelopment project.

Document Control and References

Changes history

Issue 0.1 (7/5/2003): First draft, for internal review. Derived from [2].

Issue 1.0 (19/8/2008): Updated for public release.

Changes forecast

Update after internal review, then issued to client(s). No further changes forecast

Document references

1 Token ID Station (TIS) Kernel Protection Profile, version 1.0, 5th February 2003, D0205-01v10PPTISKernel.sxw, W. W. Everett

2 Security Target, S.P1229.40.1, issue 1.0