Tokeneer ID Station
Security Target

S.P1229.40.1
Issue: 1.2
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

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 Identification

There are five systems of interest:

- the operational Tokeneer system
- the operational ID Station (a component of the operational Tokeneer system)
- the re-developed ID Station (non-operational, but functionally equivalent to the operational ID Station)
- the re-developed ID Station core functions (a subset of the software in the re-developed ID Station)
- the re-developed ID Station support functions (all of the re-developed ID Station *except* the re-developed ID Station core functions)

This Security Target relates to the **re-developed ID Station**. Although the Tokeneer system itself is a working, secure system, the re-developed ID Station is only one component, and is not fully operational, in that the peripherals are modelled by simulators.

In order for this Security Target to be representative of one aimed at an operational system, it will at all stages refer to the TOE *as if* it were the operational ID Station, and then subsequently explain how the issues are altered for the re-developed ID Station.

“TOE” will refer to the re-developed ID Station as though it were operational, with real peripherals.

“Re-developed ID Station” will refer to the actual implementation of the re-developed ID Station.

This security target is based on the Protection Profile given in [1]. Most sections refer out to [1], and then list the explicit exclusions.

1.3 CC Conformance

No formal evaluation is being carried out, and no claims of security are being made. However, the development of the **re-developed ID Station** is intended to indicate the processes necessary for the TOE to conform to:

- **Protection Profile [1]** (excluding those areas specifically identified in the remainder of this security target)

In addition, the development of the **re-developed ID Station core functions** is intended to indicate the processes necessary for the TOE to conform to:

- **Package EAL5**

2 TOE Description

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

1 The TOE controls only the entry to the secure enclave, not the egress. There is no exit station, and no exit functionality.

2 No keypad is provided — only two-factor authentication is supported.

3 The Voice box does not form part of the TOE.

4 The TOE manages a single portal, not multiple portals.

5 No certificate revocation lists (CRLs) are supported.

6 Communications between peripherals and the central unit of the TOE are assumed protected by other means, and no technical secure communications is provided.

7 No replay protection on the biometric device is supported.

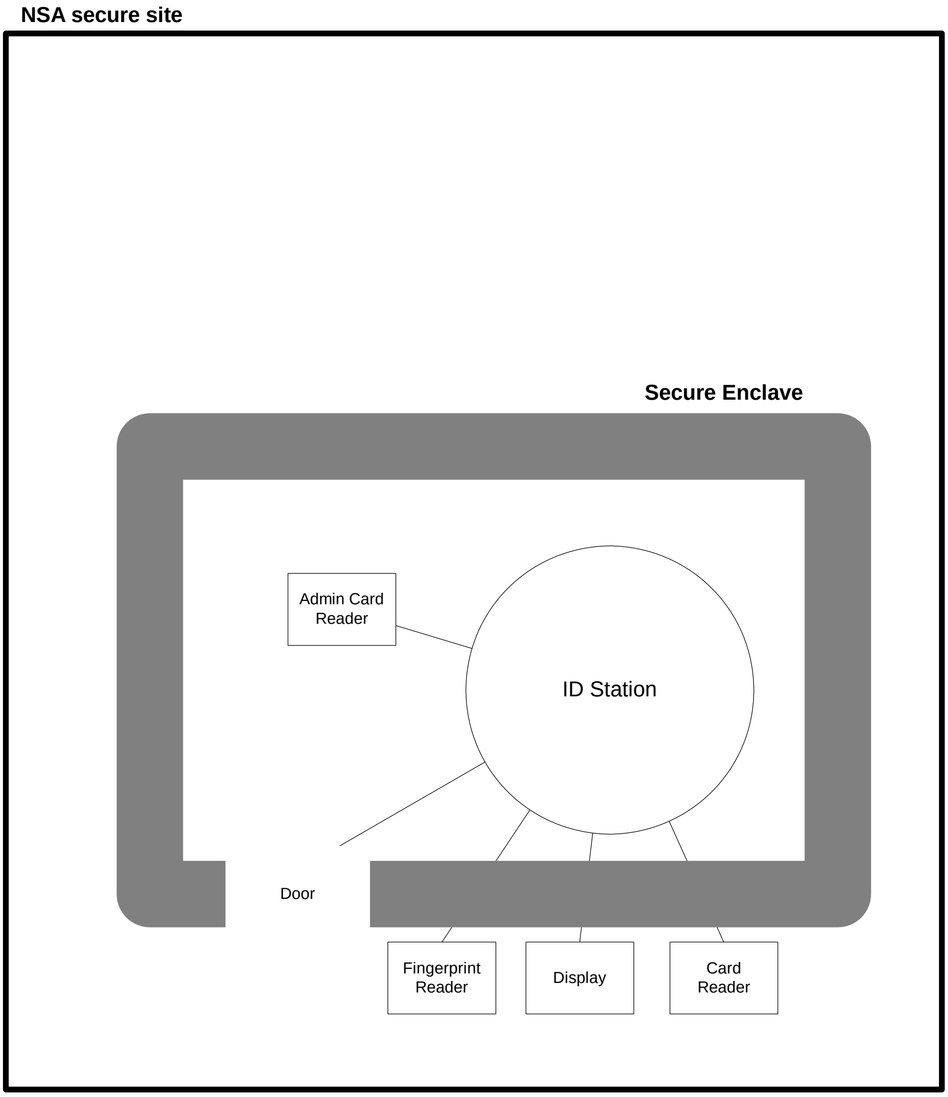
8 Internal integrity checks, manual integrity checks, diagnostics and decommissioning are not supported.

9 No backup or restore is supported.

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

3 TOE Security Environment

All of the TOE resides within a secure area within the NSA main site. Within this area there is also a Secure Enclave. The main part of the TOE is also within this Secure Enclave – only some of the peripherals (card reader, display, fingerprint reader) are outside. The door latching mechanism is on the boundary of the Secure Enclave.



3.1 Assumptions

The TOE will be used as part of the Tokeneer system to control entry to the Secure Enclave and to control logon to the Workstations within the Secure Enclave.

The area is high security. All of the people will have been security cleared, some as part of their employment by the NSA and the rest by virtue of being visitors to the site. This means that none of the people will have malicious attack intent, and the security measures will be to prevent unintentional unauthorised access to the Secure Enclave or the Workstations.

The assumptions in section 3.1 of [1] are assumed.

3.2 Threats

A full threat and vulnerability analysis should be carried out for the TOE, but will not be done for this research re-development project as is out of scope.

The work would involve analysis of the current and envisaged specific environment of the ID Station, the profile of the people with access to it, and the sensitivity of the assets being protected. It would also investigate the design of the Tokeneer system, looking for ways in which it is open to attack. The result of the threat and vulnerability analysis would inform and justify the development of the security objectives given in section 4.

The Protection Profile [1] presents a generic threat analysis, to which this TOE conforms.

3.3 Organisational Security Policies

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

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 this redevelopment project.

P.Availability

Availability is out of scope of this redevelopment project.

DP.Screen_Locking

No GUI is being developed, and no requirements on the GUI are in scope.

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 out of scope of this redevelopment project.

P.Marking

There are no outputs, and marking is not relevant.

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.

4 Security Objectives

4.1 Security Objectives for the TOE

The TOE has two primary objectives:

- To prevent accidental, unauthorised access to the Secure Enclave.
- To prevent accidental, unauthorised access to any of the Workstations within the Secure Enclave.

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

O.Audit_Account

No audit analysis or presentation functionality is supported. Audit archiving is the only facility to allow audit to be inspected.

O.Code_Signing

There is no downloaded code. Installation is manual and not covered by technical security.

O.Crypto_Data_Sep

Due to the simulation of the cryptographic module, this cannot be guaranteed.

O.Crypto_Import_Export

Due to the simulation of the cryptographic module, this cannot be guaranteed.

O.Crypto_Key_Man

Due to the simulation of the cryptographic module, this cannot be guaranteed.

O.Crypto_Self_Test

No self-test or integrity checking is in scope of this redevelopment project.

O.External_Labels

No data is exported to external systems, apart from the information written to the Token.

O.Fault_Tolerance

No self-test or integrity checking is in scope of this redevelopment project.

O.General_Integ_Checks

No self-test or integrity checking is in scope of this redevelopment project.

O.I&A_Transaction

Audit will record actions at a sufficient level of detail.

O.Identify_Unusual_Act

No self-test or integrity checking is in scope of this redevelopment project.

O.Info_Flow_Control

There are no security issues to do with information flow.

O.Integ_Sys_Dat_Int

No self-test or integrity checking is in scope of this redevelopment project.

O.Integrity_Data/SW

No self-test or integrity checking is in scope of this redevelopment project.

O.Integrity_Data_Rep

No self-test or integrity checking is in scope of this redevelopment project.

O.Integrity_Practice

No self-test or integrity checking is in scope of this redevelopment project.

O.Screen_Lock

No GUI is being developed, and no requirements on the GUI are in scope.

O.Storage_Integrity

No self-test or integrity checking is in scope of this redevelopment project.

O.Sys_Access_Banners

No GUI is being developed, and no requirements on the GUI are in scope.

O.Sys_Backup_Procs

Backup and restore is not within scope for this redevelopment project.

O.Sys_Backup_Restore

Backup and restore is not within scope for this redevelopment project.

O.Sys_Backup_Storage

Backup and restore is not within scope for this redevelopment project.

O.Sys_Backup_Verify

Backup and restore is not within scope for this redevelopment project.

O.Sys_Self_Protection

No self-test or integrity checking is in scope of this redevelopment project.

O.Tamper_ID

No self-test or integrity checking is in scope of this redevelopment project.

O.Trusted_DS_Recover

No self-test or integrity checking is in scope of this redevelopment project.

O.Trusted_Recovery

No self-test or integrity checking is in scope of this redevelopment project.

O.Trusted_Recovery_Doc

No self-test or integrity checking is in scope of this redevelopment project.

O.User_Data_Integrity

No self-test or integrity checking is in scope of this redevelopment project.

4.2 Security Objectives for the Environment

To allow the TOE to successfully satisfy its security objectives, the environment must achieve the following objectives:

- To secure the Secure Enclave against entry to any person *except* to a person
  - who presents themselves for authentication at the TOE; and
  - for which the TOE has unlocked the door to the enclave.
- To ensure that the Workstations are accessible only to people *physically within* the Secure Enclave.
- To protect the Secure Enclave and the surrounding area from any malicious physical attack, including any physical attack on the TOE.

- To protect any person presenting themselves for entry to the Secure Enclave from interference (such as theft of their Token, coercion in the use of the biometric device, passing through the door by someone else, etc.).

The statements of section 4.2 of [1] all apply.

5 IT Security Requirements

5.1 TOE Security Requirements

5.1.1 TOE Security Functional Requirements

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

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.

SFP.Digital_Signing

Cryptography will be simulated.

In FAU_GEN.1, delete the following auditable events (these are all deleted due to the non-support of the associated functions):

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

FAU_SAR.1

The Auditor will be able to export the audit archive, but all viewing and analysis functions will be done externally.

FAU_SAR.2

The Auditor will be able to export the audit archive, but all viewing and analysis functions will be done externally.

FAU_SAR.3

The Auditor will be able to export the audit archive, but all viewing and analysis functions will be done externally.

FAU_STG.2.1

No self-test or integrity checking is in scope of this redevelopment project.

FAU_STG.2.2

No self-test or integrity checking is in scope of this redevelopment project.

FCS_CKM.1

No cryptographic key operations are implemented, as all cryptographic aspects are simulated.

FCS_CKM.2

No cryptographic key operations are implemented, as all cryptographic aspects are simulated.

FCS_CKM.3

No cryptographic key operations are implemented, as all cryptographic aspects are simulated.

FCS_CKM.4

No cryptographic key operations are implemented, as all cryptographic aspects are simulated.

FCS_COP.1

No cryptographic key operations are implemented, as all cryptographic aspects are simulated.

FDP_ETC.2

No secure data is being exported.

FPD_IFC.2

There are no security issues to do with information flow.

FDP_IFF.2

There are no security issues to do with information flow.

FDP_ITC.1

No user data is being imported.

FDP_ITC.2

No user data is being imported.

FDP_SDI.1

No self-test or integrity checking is in scope of this redevelopment project.

FIA_AFL.1

For two-factor authentication where failure relates only to invalid token certificates and biometric readings, rather than forgotten PINs are attempts at guessing a PIN, a limit on the number of retries makes less sense.

FIA_ATD.1

The core functionality agreed used the Authorisation Certificate as the basis of roles and privileges. More sophisticated role assignment is therefore beyond the scope of the core functions.

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.

Under FMT_MTD.1.1, use modified table 3 instead.

FMT_REV.1

No revocation is supported.

FMT_SMR.2.3

Decommissioning is not supported.

FPT_AMT.1

No self-test or integrity checking is in scope of this redevelopment project.

FPT_ITT.2

No self-test or integrity checking is in scope of this redevelopment project.

FPT_ITT.3

No self-test or integrity checking is in scope of this redevelopment project.

FPT_PHP.3

The TOE is in a secure area, and no protection against physical attack is required.

FPT_RCV.2

No self-test or integrity checking is in scope of this redevelopment project.

FPT_RCV.4

No self-test or integrity checking is in scope of this redevelopment project.

FPT_RPL.1

Replay protection is not within scope of this redevelopment project.

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.

FPT_TRC.1

No self-test or integrity checking is in scope of this redevelopment project.

FPT_TST.1

No self-test or integrity checking is in scope of this redevelopment project.

FRU_FLT.2

No self-test or integrity checking is in scope of this redevelopment project.

FTA_SSL.1

No GUI is being developed, and no requirements on the GUI are in scope.

FTA_SSL.2

No GUI is being developed, and no requirements on the GUI are in scope.

FTA_TAB.1

No GUI is being developed, and no requirements on the GUI are in scope.

FTA_TSE.1

No revocation lists are supported.

5.1.2 TOE Security Assurance Requirements

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

In 5.2.6: “tests” will be taken to include SPARK analysis.

5.2.7:

AVA_CCA.1

Covert channels are not a security issue for this TOE.

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.

5.2 IT Environment Security Requirements

The statements of section 5.4 of [1] apply.

6 TOE Summary Specification

This will be presented in the Formal Functional Specification.

7 PP Claims

7.1 PP Reference

The Protection Profile given in [1] is being adhered to, apart from the exclusions listed in the body of this security target.

8 Rationale

This security target requires the TOE to conform to the Protection Profile given in [1]. The justification and rationale for the reasonableness of the security requirements can therefore be found in [1].

Document Control and References

Praxis High Integrityl Systems Limited, 20 Manvers Street, Bath BA1 1PX, UK.
Copyright © (2003) United States Government, as represented by the Director, National Security Agency. All rights reserved.

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

Changes history

Issue 0.1 (31/3/2003): First draft, for internal review.

Issue 1.0 (23/4/2003): Issue to client for review.

Issue 1.1 (13/5/2003): Minor changes due to errors found in tracing to the formal specification. Issued with change bars.

Issue 1.2 (19/8/2008): Updated for public release.

Changes forecast

None.

Document references

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