TARANTELLA

SECURING THE FUTURE OF THE FREE ENTERPRISE

Tarantella Enterprise 3 Security Target

Issue : 2.4

Date : 11 April 2005

Status : Definitive Release

Document reference : 309.EC200409:40.1

Distribution :

Prepared by : Robert Allison &
Hugh Griffin

....

Reviewed by : Steve Hill

....

Authorised by : Andy Hall

....

This Security Target was prepared by:
LogicaCMG CLEF (LFL)
LogicaCMG UK Ltd.
Chaucer House
The Office Park
Springfield Drive
Leatherhead
Surrey KT22 7LP

On behalf of **:**
Tarantella Ltd.
Richmond House
Lawnswood Business Park
Redvers Close
Leeds
LS16 6RD

Document History

Version	Date	Notes
0.1		Initial draft
0.2	22/10/03	LogicaCMG technical review draft
0.9	24/10/03	Client Release
1.0	25/11/03	Definitive Release
1.1	27/10/03	Grammar and typo corrections by Chris Scheybeler
1.2	07/07/04	Updates in response to evaluator observations, Certifier comments and Tarantella comments
1.3	09/07/04	Incorporation of comments from LogicaCMG technical review
1.4	19/07/04	Incorporation of comments from Tarantella
1.5	06/09/04	Incorporation of comments from Certifier. Also response to OR4/3, OR4/4, and OR2/11.
2.0	13/09/04	Definitive Release
2.1	10/11/04	SOF-basic claim added
2.2	21/12/04	Hardware requirements now sparc architecture
2.4	11/4/05	Clarification of firewall usage. Updated doc properties.

Table Of Contents

1 Introduction 7
1.1 Security Target Identification 7
1.2 Security Target Overview 7
1.3 CC Conformance Claim 8
1.4 Document Structure 8

2 TOE Description 9
2.1 Product Overview 9
2.2 Evaluated Configuration 10
2.3 Summary of IT and Security Features 12

3 TOE Security Environment 13
3.1 Assumptions 13
3.2 Threats 14
3.3 Organisational Security Policies 15

4 Security Objectives 17
4.1 TOE Security Objectives 17
4.2 Security Objectives for the Environment 17

5 Security Requirements 21
5.1 Security Functional Requirements 21
5.2 Security Assurance Requirements 25
5.3 Strength of Function Claims 25
5.4 Security Requirements for the IT Environment 26

6 TOE Summary Specification 27
6.1 IT Security Functions 27
6.2 Required security mechanisms 29
6.3 Assurance Measures 29

7 ST Rationale 31
7.1 Security Objectives Rationale 31
7.2 Security Requirements Rationale 34
7.3 TOE Summary Specification Rationale 39
7.4 PP Claims Rationale 41

Abbreviations

CC	Common Criteria
CEM	Common Evaluation Methodology
CI	Configuration Item
EAL	Evaluation Assurance Level
ENS	Enterprise Name Space
ETR	Evaluation Technical Report
EWP	Evaluation Work Programme
FIPS	Federal Information Processing Standard
ISO	International Standards Organisation
ISPM	Informal Security Policy Model
IT	Information Technology
JVM	Java Virtual Machine
OR	Observation Report
OSP	Organisational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SIN	Scheme Information Notice
SOF	Strength of Function
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

Referenced Documents

CC	Common Criteria for Information Technology Security Evaluation (Comprising Parts 1-3: [CC1], [CC2], and [CC3])
CC1	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model CCIMB-2004-01-001, Version 2.2, January 2004
CC2	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements CCIMB-2004-01-002, Version 2.2, January 2004
CC3	Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements CCIMB-2004-01-003, Version 2.2, January 2004
CEM	Common Methodology for Information Technology Security Evaluation Part 2: Evaluation Methodology CEM-2004-01-004, Version 2.2, January 2004
RFC 2246	http://www.faqs.org/rfcs/rfc2246.html

This Page Intentionally Blank

1 Introduction

1.1 Security Target Identification

This document is the Security Target (ST) for Tarantella Enterprise 3, version 3.40.911 with the Tarantella Advanced Security Pack, version 3.41.211. Hereafter, referred to as either "the TOE", "Tarantella Enterprise 3" or simply "Tarantella".

Document Title	Tarantella 3 Enterprise Security Target
Version	2.4
Owner	Tarantella Ltd
Originator	LogicaCMG
TOE	Tarantella Enterprise 3, version 3.40.911 with the Tarantella Advanced Security Pack, version 3.41.211
CC Version	2.2 January 2004
Assurance Level	EAL2
Strength of Function	SOF-basic

The role of the security target within the development and evaluation process is described in the CC: the Common Criteria for Information Technology Security Evaluation [CC].

1.2 Security Target Overview

This document describes the security features of Tarantella Enterprise 3.

In particular this Security Target shows the environment in which the TOE is to operate, the threats against it and the functionality required and provided to meet these threats. It also enumerates the components of the TOE, defining its boundary and its dependencies.

The TOE provides secure web-based access to applications. It is located between the users, who run a web browser, and the server-based applications, which the TOE delivers over the Internet, an extranet or intranet. Supported back-end application servers include Microsoft Windows 2000 and 2003 Servers, RedHat Linux 3.0 and Solaris 8 or later server. (Note that these application servers and the communications with them (RDP/SSH/X11) are out of scope).

1.3 CC Conformance Claim

The TOE conforms to the CC as follows:

- CC Part 2 extended
- CC Part 3 conformant
- EAL2 conformant.

1.4 Document Structure

This ST is divided into 8 sections, as follows:

- Section 1 (this section) provides an introduction to the ST.
- Section 2 provides a description of the TOE.
- Section 3 provides the statement of TOE security environment, which defines the security problem the TOE is intended to meet.
- Section 4 provides the statement of security objectives, defining what is expected of the TOE and its environment, in order to address the security problem defined in Section 3.
- Section 5 provides the statement of IT security requirements, defining the functional and assurance requirements on the TOE (and its IT environment) that are needed to achieve the relevant security objectives defined in Section 4.
- Section 6 provides the TOE summary specification, which defines how the TOE meets the IT security requirements defined in Section 5.
- Section 7 provides the ST Rationale, which demonstrates that:
    - the security problem defined in Section 3 will be suitably addressed if the TOE and its environment meet the stated security objectives in Section 4;
    - the TOE and IT environment security objectives will be achieved if the TOE and IT environment satisfies the IT security requirements in Section 5;
    - the TOE security requirements will be met if it correctly implements the security functions and assurance measures defined in Section 6.

2 TOE Description

This section describes the TOE as an aid to the understanding of its security requirements and features. The scope and boundaries of the TOE are described in general terms both physically, in terms of hardware and software components and logically, in terms of IT security features offered by the TOE.

2.1 Product Overview

Tarantella Enterprise Server 3 provides secure, managed access to server-based applications through a Java-enabled web browser.

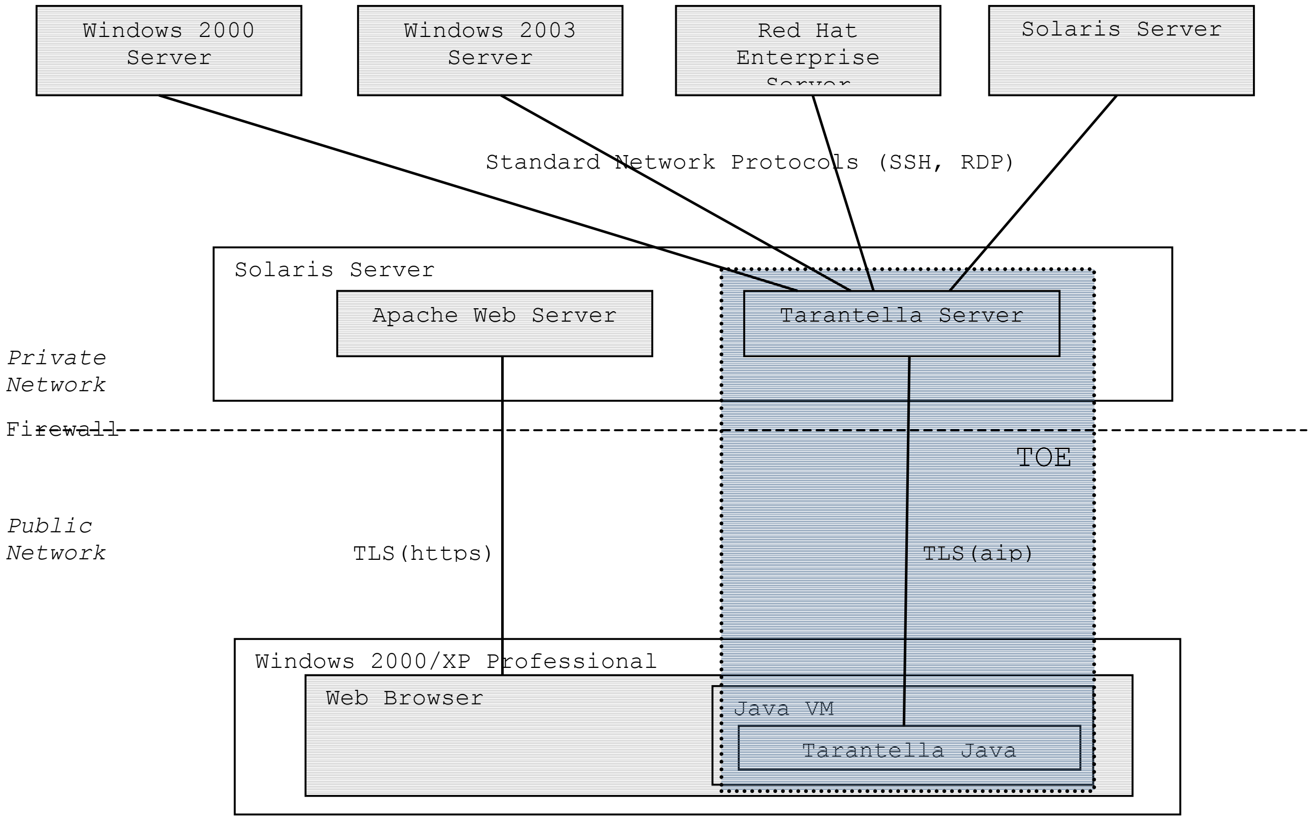

Figure 1 – Architectural Overview

Tarantella acts as a secure intermediary between the applications, running on a variety of application servers in a protected environment, and an authorized user who can work from anywhere.

The user's experience is one of:

- point the browser at the URL of the Tarantella server;
- the Tarantella client is downloaded and starts up (note that this is a function of the JVM. Typically Java archives are cached by the JVM);
- login to Tarantella server via downloaded client;
- see a list of applications which they are allowed to run (the webtop);
- single click on an application icon to launch an application on a remote server;
- a browser window is opened in which the launched application is displayed. The user interacts with the remote application as though it were running locally.
- access to local printers and drives is allowed under the control of the Administrator.
- all client-server communications are TLS-encrypted through the Tarantella Advanced Security Pack.

The administrator uses the Tarantella Object Manager administration tool to:

- create host objects representing the servers from which applications are run;
- create application objects and specify which hosts to connect to, how to connect, and how to run applications once connected;
- decide which Tarantella users have rights to run which applications.

All application access happens through the Tarantella server. This provides administrator control and knowledge of user access to applications.

2.2 Evaluated Configuration

2.2.1 Scope of the TOE

The TOE software comprises:

- Tarantella Enterprise 3 base component version 3.40.911 for Solaris 8. This contains:

  - Tarantella Enterprise 3 server
  - Tarantella Enterprise 3 Java client
  - Tarantella Enterprise 3 administration tools:
    - Tarantella Object Manager;
    - Tarantella Array Manager;
    - Tarantella Command Line Interfaces.
- Tarantella Advanced Security Pack version 3.41.211.

2.2.2 IT Environment Software requirements

The following are beyond the scope of the TOE but are required for a useful system to exist:

Tarantella Client Software

- Tarantella Client operating system – Windows XP Pro or Windows 2000 Pro;
- Internet Explorer;
- Sun Java Plug-In, version 1.4.2.

Tarantella Server Software

- Tarantella Server operating system Solaris 8;
- The UNIX authentication scheme used by Solaris 8.

Application Server Software

- Server-based platforms on which the server-based applications run – Windows 2000/2003 server, Solaris 8 or later server, and Red Hat Enterprise 3.0 server;
- Server-based applications to which Tarantella provides access.

Firewalls

- Firewalls are not required for the system to function, but often exist in the environment in which Tarantella Enterprise 3 is deployed. For this reason the configuration is such that it will operate through a firewall used to prevent direct network traffic between a public and private network.

- The firewall, if used, should be configured such that all incoming ports are blocked except a TCP connection on port 443 destined for the Tarantella Enterprise 3 server.

These firewalls are not in scope of the evaluation.

2.2.3 Hardware requirements

As part of the environment the TOE will run on any Sun Solaris compatible server based on the Sparc architecture.

For hardware server options see http://www.sun.com/servers

2.3 Summary of IT and Security Features

Tarantella provides a gateway to server-based applications. For each user, a profile is created that contains information about the applications to which the user needs access.

When a user connects to Tarantella they are required to provide a username and password. (Note that this gives access only to the Tarantella Server, and is in addition to identification given to access the Tarantella Client and the Tarantella Server Operating Systems). The Tarantella Server passes these credentials to an external authentication system for validation. (Note that this is the authentication system that Solaris 8 provides as an OS service). If successful, a virtual desktop (or webtop) is created for the user with icons for each application to which they are permitted access.

Users may then proceed to launch the applications that are displayed on their webtop. Where the applications are running on one of the application servers, the user may be prompted for further credentials, such as another username and password for that particular server, before the application is displayed. (Note that these communications to the Application Server involves a separate authentication process, which is not in scope of the TOE).

All communications between the Tarantella Client and the Tarantella Server take place over a secure Transport Layer Security (TLS) channel. TLS authenticates the Tarantella server, encrypts the data transmitted and provides applications securely across the Internet, extranet, or intranet connections.

3 TOE Security Environment

This part of the ST provides the statement of TOE security environment, which defines the security problem the TOE and its environment is intended to address.

To this end, the statement of TOE security environment identifies the assumptions made on the environment and the intended method of use of the TOE, defines the threats that the TOE is designed to counter, and the organisational security policies with which the TOE is designed to comply.

3.1 Assumptions

This part of the security problem definition scopes the security problem by identifying what aspects of the TOE security environment are taken to be axiomatic. Note that in general “Administrators of the TOE” specifically relates to “Administrators of the Tarantella Server component of the TOE”.

3.1.1 Physical assumptions

A.PHYSICAL It is assumed that the TOE and protected application servers are located in a place that can only be physically accessed by trusted personnel.

3.1.2 Personnel assumptions

A.ADMIN Administrators of the TOE are assumed to be trustworthy and competent.

3.1.3 Connectivity assumptions

A.CONNECT Administrators will correctly configure any firewalls used.

Note: the firewalls are outside the scope of the TOE.

A.CERTIFICATE The administrator will install, manage and destroy the X.509 certificate(s) used for TLS connections in a secure manner.

3.1.4 Authentication assumptions

A.AUTH It is assumed that external authentication systems provide appropriate decisions on validating the user’s username and password.

A.USER Users will keep their passwords known only to themselves.

3.1.5 Configuration Assumptions

A.CONFIG It is assumed that the following features are configured as specified:

- The Tarantella Advanced Security Pack is installed, configured and running in accordance with the evaluated configuration
- A unique “ENS person object” is created for every Tarantella user (required for login retry lockout – FIA_AFL.1)
- Only administrative users have interactive login accounts on the hosts that provide the platforms for the Tarantella Server and Application Servers
- The Firewalls are configured correctly and securely (applies to hardware and software)
- The Tarantella client, server and application server operating systems are operating correctly and configured securely.

3.2 Threats

This part of the security problem definition identifies the assets requiring protection

3.2.1 Assets requiring protection

This section defines the assets that require protection in the TOE security environment.

The principal protected assets are the applications that run on the protected application servers. Secondary to this is the data that these applications give access to.

The other protected assets are the application data in transit between Tarantella Clients and the Tarantella Server only.

3.2.2 Threat agents

Threat agents are expected to be:

- Unauthorised users
- Authorised users attempting to exceed their authorisation.

3.2.3 Statement of threats

This section provides the statement of threats to the assets that require protection.

T.UNAUTH Unauthorised users may attempt to access applications and/or application data

NOTE: this threat covers masquerade attempts by an authorised user and attempts to access another user's data in transit.

T.EXCEED Authorised users may attempt to access applications for which they are not authorised.

NOTE: an authorised user may seek to abuse their privilege on the system by accessing applications for which they have no need to use.

T.CHANNEL Communication channels may be compromised or become unreliable such that users of the TOE may believe that they are accessing the TOE when they are not. This may result in the compromise of data in transit between the Tarantella Client and Tarantella Server.

T.MISDIRECT An attacker may use malicious software to redirect communication between the Tarantella Client and Tarantella Server to another server.

3.3 Organisational Security Policies

This part of the security problem definition refines the security problem by identifying organisational policy constraints relating to the protection of the assets identified in section 3.2.1.

OSP.CRYPTO Cryptographic functions shall be validated to FIPS140-2 level 1.

Note: the implication of this is that the TOE is appropriate for use in organisations which mandate (or accept) FIPS 140-2 approved products.

This Page Intentionally Blank

4 Security Objectives

This part of the ST defines the security objectives that the TOE and its environment must meet, in order to fully address the security problem defined in Section 3. Note that in general "Administrators of the TOE" specifically relates to "Administrators of the Tarantella Server component of the TOE".

4.1 TOE Security Objectives

The TOE shall comply with the following security objectives.

O.ADMIN The TOE shall provide functionality that enables an authorised administrator to effectively manage the TOE and its security functions, and shall ensure that only authorised administrators are able to access such functionality.

O.AUDIT The TOE shall provide the means of recording any security relevant events, so as to:

a) assist an administrator in the detection of potential attacks or misconfiguration of the TOE security features that would leave the TOE susceptible to attack; and

b) hold users accountable for any actions they perform that are relevant to security.

O.DAC The TOE shall provide administrators with the means of controlling and limiting access to the objects and resources for each user, on the basis of individual users or identified groups of users.

O.I&A The TOE shall uniquely identify all users, and shall authenticate the claimed identity (via an external authentication service) before granting a user access to the system.

O.TPATH The TOE shall prevent disclosure and modification of data, by unauthorised users, during transmission of the data between its physically separate components.

O.AUTH_SERVER The Tarantella server must authenticate itself to client components before communication of sensitive data.

O.SECURE_ENCRYPTION The TOE shall use encryption modules validated to FIPS140-2.

4.2 Security Objectives for the Environment

4.2.1 IT Environment Security Objectives

The IT environment shall comply with the following security objectives.

OE.OSAUTH The underlying operating system shall uniquely identify all administrators, and shall authenticate the claimed identity before granting an administrator access to the system.

OE.AUDREC The Tarantella Server, in conjunction with the underlying operating system, will provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.

OE.OSKEYS The underlying operating system shall provide the capability to import the X.509 certificate keys without security attributes.

4.2.2 Non-IT Environment Security Objectives

The environment shall comply with the following security objectives.

OE.OSCONFIG Administrators shall ensure that the operating systems on the Tarantella clients, servers and application servers are configured securely.

The operating system used for the Tarantella server shall be Solaris 8.

The operating systems used for Tarantella application servers shall be limited to:

- Windows 2000 Server,
- Windows 2003 Server,
- RedHat Enterprise Linux 3.0,
- Solaris 8 or later server.

The operating systems that are used for the Tarantella clients shall be limited to:

- Windows XP Pro,
- Windows 2000 Pro.

OE.ACCOUNT Administrators of the TOE shall ensure that:

a) The TOE is configured such that only the approved group of users for which the system was accredited may access the system

b) Each individual user is assigned a unique user ID – a Tarantella user object.

OE.AUDMAN Administrators of the TOE shall ensure that the audit functionality is used and managed effectively. In particular:

a) Procedures shall exist to ensure that the audit trail is regularly analysed and archived, to allow retrospective inspection.

b) The auditing system must be configured such that the loss of audit data is minimised upon:

i. planned or unplanned shutdown; or

ii. lack of available audit storage.

c) The media on which audit data is stored must not be physically removable from the server by unauthorised users.

OE.AUTHDATA Those responsible for the TOE shall ensure that user authentication data is stored and processed securely and not disclosed to unauthorised individuals. In particular:

a) Procedures shall be established to ensure that user passwords generated by a trusted role during user account creation or modification are distributed in a secure manner.

b) The media on which authentication data is stored shall not be physically removable from the server by unauthorised users.

c) Users shall not disclose their passwords to other individuals.

OE.INSTALL Those responsible for the TOE shall establish and implement procedures to ensure that the hardware, software and firmware components that comprise the networked product are distributed, installed and configured in a secure manner within secured physical locations. This entails the following configuration on the TOE:

- Anonymous logins are not used;
- Shared/guest logins are not used;
- Access to files on Tarantella clients is not permitted.

OE.KEYMGMT Those responsible for the TOE environment will ensure that X.509 certificates used by the TOE are procured and managed in manner that prevents their unauthorised disclosure.

This Page Intentionally Blank

5 Security Requirements

This part of the ST defines the security requirements that the TOE and its IT environment must meet in order to achieve the corresponding security objectives defined in Section 4. Requirements for the TOE are divided in to Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs). The CC requires that these be constructed, where possible, using security functional and assurance components defined, respectively, in [CC2] and [CC3].

This section also states the strength of TOE security function claims (SOF).

5.1 Security Functional Requirements

The following table provides a summary of the Security Functional Requirements (SFRs) implemented in the TOE from CC Part 2 [CC2]:

Component	Name
FIA_UID.2	User identification
FIA_UAU.2	User authentication
FIA_UAU.5	User authentication
FIA_UAU.7	User authentication
FIA_AFL.1	Authentication failures
FMT_SMR.1	Security management roles
FAU_GEN.1	Security audit data generation
FAU_GEN.2	Security audit data generation
FAU_SAR.1	Security audit review
FAU_SAR.2	Security audit review
FAU_SAR.3	Selectable audit review
FAU_STG.1	Security audit event storage
FDP_RIP.2.1	Residual information protection
FDP_ACC.2	Access control policy

Component	Name
FDP_ACF.1	Access control functions
FMT_MSA.1	Management of security attributes
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FPT_ITT.1	Internal TOE TSF data transfer
FPT_ITT.3	Internal TOE TSF data transfer
FCS_COP.1	Cryptographic operation

Table 5.1 Security Functional Requirement Summary

The following typographic conventions are used to identify the operations performed on the SFRs:

- Assignments and selections are shown in *italics*.
- Refinements are shown in **bold**.

5.1.1 Identification and Authentication

Note: the TOE makes calls to underlying authentication mechanisms that actually perform the authentication process and feedback the result. The underlying mechanisms themselves are outside the scope of the TOE.

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.5.1 The TSF shall provide *the UNIX authentication interface to a user* to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the *UNIX authentication mechanism*.

Note: [CC2] uses FIA_UAU.5 for defining multiple authentication mechanisms. It is used in this security target to identify the single authentication mechanism used by the TOE.

FIA_UAU.7.1 The TSF shall provide **no feedback other than success or failure** to the user while the authentication is in progress.

FIA_AFL.1.1 The TSF shall detect when *three* unsuccessful authentication attempts occur related to *user login*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall *lock the user account on the specific Tarantella server used.*

Note FIA_AFL.1 only applies when there is an ENS person object for every user of Tarantella. When an account is locked, it is only locked in Tarantella, the account may still be used to login to the operating system.

FMT_SMR.1.1 The TSF shall maintain the roles *user and administrator*.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.2 Audit and Accountability

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) Start and end of a user application session.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, *the application accessed by the user*.

Note: a user may access a number of applications during one session on the TOE.

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1.1 The TSF shall provide *administrators* with the capability to read all *accounting information* from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the **administrator** to interpret the information.

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those **administrative** users that have been granted explicit read-access.

FAU_SAR.3.1 The TSF shall provide the ability to perform *searches* of audit data based *on the following attributes:*

a) User identity,

b) *Application used,*

c) *Time of application access.*

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to *prevent* unauthorised modifications to the audit records in the audit trail.

5.1.3 Object Re-use

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource* to all objects.

5.1.4 Access Control

FDP_ACC.2.1 The TSF shall enforce the *User access control SFP* on users and *the applications to which they are granted access* and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

FDP_ACF.1.1 The TSF shall enforce the *User access control SFP* to objects based on *user security attributes*.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) *The user has been granted authorisation to execute the application;*

b) *A user requesting access to an administrative function has an administrative role.*

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on *the following additional rules: none.*

FMT_MSA.1.1 The TSF shall enforce the *User access control SFP* to restrict the ability to *modify* the following security attributes to *administrative users*:

a) *Applications available to users via their webtop*

b) *User role.*

FMT_MTD.1.1 The TSF shall restrict the ability to *create, modify, delete the list of available applications* to *administrators*.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

a) *create, modify, delete the list of applications available to users;*

b) *modify the user role;*

c) *modify the set of auditable events.*

FTP_ITC.X.1[1] The TSF shall provide a communication channel between **the Tarantella client and Tarantella server** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.X.2 The TSF shall permit *the Tarantella client* to initiate communication via the trusted channel.

FTP_ITC.X.3 The TSF shall initiate communication via the trusted channel for *authentication of the Tarantella server and all communication*.

FPT_ITT.1.1 The TSF shall protect TSF data from *disclosure and modification* when it is transmitted between separate parts of the TOE.

FPT_ITT.3.1 The TSF shall be able to detect *modification of data* for TSF data transmitted between separate parts of the TOE.

FPT_ITT.3.2 Upon detection of a data integrity error, the TSF shall *drop the connection.*

FCS_COP.1.1 The TSF shall perform *encryption of the data stream between the client and server components* in accordance with the specified cryptographic algorithm *3DES as defined by the ciphersuite RSA_WITH_3DES_EDE_CBC_SHA in the TLS specification in [RFC 2246]* and cryptographic key size *168 bit* that meet *FIPS140-2, level 1*.

5.2 Security Assurance Requirements

The target evaluation assurance level for the product is EAL2 [CC3]. No augmented assurance requirements are included.

5.3 Strength of Function Claims

A claim of SOF-basic is made for Strength of Function.

The strength of cryptographic algorithms is outside the scope of the CC, and hence the assessment of algorithmic strength will not form part of the TOE evaluation.

[1] Note that this is an extended component as the client-server relationship within the TOE does not fit into the TSF to remote trusted IT product paradigm of the [CC2] component.

The TOE does not contain any probabilistic or permutational mechanisms - the TOE itself does not implement the authentication mechanisms, but relies on the IT environment, and is responsible for enforcing those decisions.

The EAL2 assurance level implies through the AVA_VLA.1 assurance component that the TOE is required to provide defence against attackers exploiting obvious vulnerabilities in the intended environment of the TOE. A claim of SOF-basic would be appropriate for this use, as it would demonstrate that obvious vulnerabilities have been addressed.

5.4 Security Requirements for the IT Environment

Tarantella relies on services provided by the underlying operating system to aid many of its security decisions and implement security services jointly as part of the security functional requirements defined in Section 5.1. This applies specifically for the following areas:

- Identification and Authentication: FIA_UID.2, FIA_UAU.2, FIA_UAU.5, FIA_UAU.7 and FIA_AFL.1. The operating system is trusted to provide interfaces for authentication and be able to provide an authentication decision to the TOE.

- Audit: FAU_GEN.1 and FAU_GEN.2. The audit files for the TOE are stored and protected by the operating system file system.

Additionally, Tarantella relies on the underlying operating system to provide:

- Import of keys: FDP_ITC.1. The administrator is required to provide X.509 certificates for use in the TOE (see A.CERTIFICATE). Note that the dependencies on this security requirement are not relevant since the operating system for the TOE is only required to provide the capacity to import these keys without security attributes, as refined in the following:

  FDP_ITC.1.1 The TSF shall enforce the *Import of keys SFP* when importing **keys** controlled under the SFP, from outside the TSC.

  FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the **keys** when imported from outside the TSC.

  FDP_ITC.1.3 The TSF shall enforce the following rules when importing **keys** controlled under the SFP from outside the TSC: *none.*

- Reliable time stamps: FPT_STM.1. The audit system of the TOE relies on the underlying operating system to provide both accurate dates and times for accounting records.

  FPT_STM.1.1 The TSF shall be able to provide reliable timestamps for its own use.

6 TOE Summary Specification

This section defines the IT Security Functions (SFs) and assurance measures that meet the TOE SFRs and SARs defined in Section 5.

6.1 IT Security Functions

6.1.1 Identification and Authentication

IA.1 When a user connects to the Tarantella Server (for example by following a link from a web page), they will be required to identify and authenticate themselves before they can access their webtop or perform any other actions mediated by the TOE.

IA.2 User authentication on the TOE is provided by the UNIX authentication interface.

IA.3 A user must authenticate as either an administrator or a webtop user.

IA.4 The TOE provides no feedback to the user during authentication other than success or failure of their attempt.

IA.5 If three consecutive authentication attempts to access a given user account fail, the TOE locks the Tarantella account for that user.

IA.6 The Tarantella Server component shall authenticate itself to client components before any sensitive data is transmitted between them.

6.1.2 Audit and Accountability

AUD.1 The TOE is able to maintain logs of the following interactions between itself and users based on the pre-selection specified in AUD.4:

a) user login,

b) user logoff,

c) application launch,

d) application close,

e) start up of the audit function,

f) close down of the audit function.

AUD.2 The TOE audit logs are stored on the host operating system.

AUD.3 Each audit log record stored on the TOE shall include at least the following information:

a) date and time of event,

b) type of event,

c) user identity,

d) the success or failure of the event,

e) based on the type of event: the application accessed by the user.

AUD.4 The TOE provides a feature that enables an administrator to query the audit trail based on the following attributes:

a) User name,

b) Application name,

c) Application launch time.

6.1.3 Object Re-use

OBJ.1 When a user logs in they are presented with a webtop. The webtop will not contain any information or application from a previous user's session.

6.1.4 Access Control

AC.1 Webtop users will only be able to access the applications that are on their Tarantella client webtop.

AC.2 The set of applications available to a user will be determined by their user identity and organisational unit as stored in the Tarantella datastore.

(Note that a Tarantella organisational unit is an internal Tarantella structure used to group Tarantella users into a hierarchy. Deploying Tarantella application objects can be performed to Tarantella users or Tarantella organisational units.)

AC.3 Only the operating system super-user account can access or delete the audit logs.

AC.4 Only Tarantella Global Administrators can create and modify TOE user accounts.

AC.5 Only Tarantella Global Administrators can change a user's webtop and the applications that a user is permitted to access.

AC.6 All sensitive data communication between the Tarantella client and the Tarantella server is encrypted using FIPS 140-2 approved crypto modules and algorithms.

AC.7 The TOE shall detect any compromise to the integrity of data transmitted between Tarantella clients and the Tarantella server.

AC.8 In the event that a compromise as specified in AC.7 is detected, the TOE shall drop the connection(s) affected.

6.2 Required security mechanisms

6.2.1 Strength of Function Claim for Security Functions

As stated in Section 5.3 the SOF claim is SOF-basic for the overall TOE. The SOF-basic claim is specifically applicable to IT security function IA.2, but note the TOE itself does not implement the authentication mechanisms, but relies on the IT environment, and is responsible for enforcing those decisions.

Note that the strength of cryptographic algorithms is outside the scope of the CC, and hence the assessment of algorithmic strength will not form part of the TOE evaluation.

6.3 Assurance Measures

Assurance Requirement	Assurance Measure
ACM_CAP.2	Configuration Management documentation will be provided
ADO_DEL.1	Delivery procedures will be provided
ADO_IGS.1	Installation, generation and start-up procedures will be provided
ADV_FSP.1	A functional specification will be provided
ADV_HLD.1	High-level design documentation will be provided
ADV_RCR.1	Representation correspondence will be evident in the relevant TSF representations
AGD_ADM.1	Administrator guidance documentation will be provided
AGD_USR.1	User guidance documentation will be provided
ALC_DVS.1	Development security documentation will be provided
ATE_COV.1	A test coverage analysis will be provided

Assurance Requirement	Assurance Measure
ATE_FUN.1	Test documentation will be provided
ATE_IND.2	No specific assurance measure, although access will be provided to the TOE in its evaluated configuration for evaluator testing
AVA_SOF.1	A SOF analysis will be provided
AVA_VLA.1	A developer vulnerability analysis will be provided. Access will also be provided to the TOE in its evaluated configuration for penetration testing

Table 6-1: Assurance Measures

7 ST Rationale

This section provides the rationale for the choice of security objectives, security requirements, and IT security functions and assurance measures, demonstrating that they are necessary and sufficient to meet the security problem as defined in Section 3. This comprises the following parts:

- the security objectives rationale, demonstrating that the security problem defined in Section 3 will be suitably addressed if the TOE and its environment meet the stated security objectives in Section 4;

- the security requirements rationale, demonstrating that the TOE and IT environment security objectives will be achieved if the TOE and IT environment satisfy the IT security requirements in Section 5;

- the TOE summary specification rationale, demonstrating that the TOE security requirements will be met if it correctly implements the security functions and assurance measures defined in Section 6.

7.1 Security Objectives Rationale

7.1.1 Suitability to counter the threats

Threat	Countered by objectives
T.UNAUTH	O.I&A, O.TPATH, OE.AUTHDATA, OE.KEYMGMT, OE.OSKEYS
T.EXCEED	O.I&A, O.ADMIN, O.AUDIT, O.DAC, OE.ACCOUNT, OE.AUDMAN, OE.AUDREC, OE.INSTALL, OE.OSAUTH, OE.KEYMGMT, OE.OSKEYS, OE.OSCONFIG
T.CHANNEL	O.TPATH, O.SECURE_ENCRYPTION, O.DAC, OE.KEYMGMT, OE.OSKEYS, OE.INSTALL
T.MISDIRECT	O.TPATH, O.DAC, O.AUTH_SERVER, OE.KEYMGMT, OE.OSKEYS

Table 7.1 Threat Suitability

T.UNAUTH

The TOE requiring all users to be uniquely identified and authenticated (O.I&A) counters the threat of unauthorised users accessing protected assets. This is supported by the objective of protecting authentication information (OE.AUTHDATA) from access (*ie* preventing use of stolen credentials). O.TPATH (supported by OE.KEYMGMT and OE.OSKEYS) prevents unauthorised users from accessing or modifying protected assets while data is being transmitted between separate physical components of the TOE.

T.EXCEED

O.I&A establishes the identity of users and hence what they are authorised to access via O.DAC. O.ADMIN and OE.ACCOUNT allow only administrators to modify what users are able to access. OE.AUDMAN, OE.AUDREC and O.AUDIT provide for records of actions performed by users, and hence the potential to detect violations.

OE.INSTALL, OE.OSCONFIG, OE.KEYMGMT and OE.OSKEYS ensure that the TOE is installed and maintained securely.

Users may also login to the host that provides the platform for the TOE; OE.OSAUTH ensures that only administrators can perform administrative functions through this interface.

T.CHANNEL

O.TPATH and O.SECURE_ENCRYPTION ensure that data can not be compromised or modified sensibly in transit between the physically separate components in the TOE network. O.DAC, OE.KEYMGMT and OE.OSKEYS support this functionality by ensuring that encryption keys are protected from unauthorised disclosure and securely managed by those administrating the TOE.

OE.INSTALL ensures that the hardware and software components of the TOE are installed and configured in a secure manner.

T.MISDIRECT

O.AUTH_SERVER and O.TPATH prevent disclosure or modification of TOE data even if data can be redirected or sent on to a server outside the TOE network by malicious software. O.DAC, OE.KEYMGMT and OE.OSKEYS support this functionality by ensuring that encryption keys are protected from unauthorised disclosure and securely managed by those administrating the TOE.

7.1.2 Suitability to meet the OSPs

OSP	Objective	Justification
OSP.CRYPTO	O.SECURE_ENCRYPTION	Self evident

7.1.3 Suitability to uphold the assumptions

Assumption	Objective	Justification
A.PHYSICAL	OE.INSTALL	The installation must be performed and maintained securely and the TOE be in locations that are sufficiently physically secure.
A.ADMIN	OE.ACCOUNT	Administrators have the ability to create any users, including administrators. They must therefore be trusted to create and configure accounts in accordance with the needs of a particular installation.
A.CONNECT	OE.INSTALL	The host that acts as a platform for the TOE may be subject to a number of possible attacks that could subsequently undermine the TOE. These potential attacks must be defended against by the installation and long-term operation of the TOE environment.
A.CERTIFICATE	OE.INSTALL	X.509 certificates are used to provide the keys securing the connections between TOE components. These must be installed so that the keys remain secure before they are used in the TOE and destroyed after expiry.
A.AUTH	OE.ACCOUNT	The objective of controlling who has access is dependent on decisions that are made by authentication schemes that are outside the scope of the TOE.
A.USER	OE.AUTHDATA	Those responsible for the TOE ensure that users know not to disclose their

Assumption	Objective	Justification
		passwords to others.
A.CONFIG	OE.INSTALL	It is assumed that the installation is configured as required for all the SFRs to be upheld.

Table 7.2 Mapping of Security Objectives to Assumptions

7.2 Security Requirements Rationale

7.2.1 Suitability to achieve the IT security objectives

Objective	Requirement	Justification
O.ADMIN	FIA_UAU.5	Ensures that only an administrator can assign an authentication method to a user.
	FMT_SMR.1 FMT_MSA.1 FMT_MTD.1 FMT_SMF.1	Requires that the TOE assign a user a role of either user or administrator. Ensures that certain functions and settings are restricted to the administrator role only.
	FAU_STG.1 FAU_SAR.1 FAU_SAR.2	Ensures that the TOE audit records are protected from non-administrator access and provides capability to review/analyse the audit data.
	FDP_ACC.2 FDP_ACF.1	Ensures that administrative privilege access controls are applied consistently.
O.AUDIT	FAU_GEN.1 FAU_GEN.2	Requires the TOE to generate appropriate information about security relevant events.

Objective	Requirement	Justification
	FAU_STG.1 FAU_SAR.1 FAU_SAR.2	Ensures that the TOE audit records are protected from unauthorised access and provides capability to review/analyse the audit data.
	FAU_SAR.3	Allows audit records to be searched on the basis of certain attributes.
O.DAC	FDP_ACC.2 FDP_ACF.1	Requires a consistent access control policy to be applied in terms of user security attributes.
	FMT_MSA.1	Requires that only administrators be permitted to change user security attributes.
	FDP_RIP.2	Ensures data handled by the TOE in memory is not inadvertently released to unauthorised subjects.
O.I&A	FIA_UID.2 FIA_UAU.2	Requires a user of the TOE to identify and authenticate prior to use of facilities.
	FIA_UAU.5 FIA_UAU.7	Identifies the methods by which an administrator may require a user to authenticate, and requires that only appropriate feedback be given to a user during authentication.
	FIA_AFL.1	Ensures the TOE locks a user account after three consecutive login failures.

Objective	Requirement	Justification
	FMT_SMR.1	Ensures the TOE associates users with either an administrative or normal user role.
O.TPATH O.SECURE_ENCRYPTION	FCS_COP.1 FPT_ITC.X	Ensures that data transmitted between physically separate parts of the TOE is encrypted to prevent disclosure.
	FPT_ITT.1 FPT_ITT.3	Requires protection of the data from modification when transmitted between separate parts of the TOE. If an error is detected, the connection to the TOE is dropped.
O.AUTH_SERVER	FPT_ITC.X	This requirement identifies the setting up of an end to end trusted link between the Tarantella client and server. In particular, FPT_ITC.X.2 and 3 require that the Tarantella server initiate this link and authenticate itself to the client.

Table 7.3 Mapping of Security Functional Requirements to Objectives

7.2.2 Security requirements for the IT environment justification

Objective	Requirement	Justification
OE.OSAUTH	FIA_UID.2 FIA_UAU.2 FIA_UAU.5 FIA_UAU.7 FIA_AFL.1	The operating system is trusted to provide interfaces for authentication and be able to provide authentication decisions to the TOE.
OE.AUDREC	FAU_GEN.1 FAU_GEN.2 FPT_STM.1	FPT_STM.1 ensures that the underlying operating system is able to provide the Tarantella Server with reliable time stamps for stamping audit records. FAU_GEN.1 and FAU_GEN.2 ensure that the audit files for the TOE are stored and protected by the operating system file system. The other elements of this objective are provided by the TOE. The rationale for O.AUDIT (in Section 7.2.1) handles the aspects provided by the TOE.
OE.OSKEYS	FDP_ITC.1	Ensures that the operating system for the TOE provides the capability to import the X.509 certificate keys without security attributes.

Table 7.4 Mapping of Security Requirements for the IT environment to Security Objectives for the IT environment

7.2.3 Dependency and Mutual Support Analysis

Requirement	Dependency	Justification
FAU_GEN.1	FPT_STM.1	Section 5.4
FAU_GEN.2	FIA_UID.1	Section 5.1.1
	FAU_GEN.1	Section 5.1.2
FIA_UAU.2	FIA_UAU.1	Satisfied by FIA_UAU.2, Section 5.1.1
FIA_UAU.7	FIA_UAU.1	Satisfied by FIA_UAU.2, Section 5.1.1

Requirement	Dependency	Justification
FIA_AFL.1	FIA_UID.1	Satisfied by FIA_UID.2, Section 5.1.1
FMT_SMR.1	FIA_UID.1	Satisfied by FIA_UID.2, Section 5.1.1
FAU_SAR.1	FAU_GEN.1	Section 5.1.2
FAU_SAR.2	FAU_SAR.1	Section 5.1.2
FAU_SAR.3	FAU_SAR.1	Section 5.1.2
FAU_STG.1	FAU_GEN.1	Section 5.1.2
FDP_ACC.2	FDP_ACF.1	Section 5.1.4
FDP_ACF.1	FDP_ACC.1	Satisfied by FDP_ACC.2, Section 5.1.4
	FMT_MSA.3	Only explicit assignments of users to applications and roles are required within the TOE. The concept of requiring default values for newly created information objects does not exist. Therefore, this dependency is not applicable.
FMT_MTD.1	FMT_SMR.1	Section 5.1.1
	FMT_SMF.1	Section 5.1.4
FPT_ITT.3	FPT_ITT.1	Section 5.1.4
FMT_MSA.1	FDP_ACC.1	Satisfied by FDP_ACC.2, Section 5.1.4
	FMT_SMR.1	Section 5.1.1
	FMT_SMF.1	Section 5.1.4
FCS_COP.1	FDP_ITC.1	Satisfied by the IT environment of the

Requirement	Dependency	Justification
		TOE. See section 5.4.

Table 7.5 Requirement Dependencies

The following SFRs have no dependencies: FIA_UID.2, FIA_UAU.5, FPT_STM.1, FDP_RIP.2, FPT_ITC.2 and FPT_ITT.1.

All dependencies of SARs are satisfied because they collectively comprise the EAL2 assurance package, with no augmentations. EAL2 is a self-contained package.

In addition to the above dependencies, mutual support between the TOE SFRs is provided as follows:

- The principal security functionality of the TOE is provided by FDP_ACC.1/ACF.1, which provide the access control policy from users to applications. The FMT SFRs support this by providing certain management functions and providing them to administrators only.
- These principal functions are supported by the FIA SFRs (UIA.2, UAU.2/5/ and 7) which provide authenticated user identities on the basis of which security access control decisions are made.
- The FPT.* and FCS.* SFRs provide support by preventing modification or access to information as it is transmitted between TOE components. FDP_RIP.2.1 provides prevention of access to information accessed during a previous user session.
- FAU.* provides support by recording the use of applications by users so that any unauthorised attempts to access applications are detected.

7.3 TOE Summary Specification Rationale

7.3.1 Suitability of the IT Security Functions

Requirement	Security Function	Justification
FIA_UID.2.1	IA.1	Self-evident
FIA_UAU.2.1	IA.1	Self-evident
FIA_UAU.5.1	IA.2	Self-evident
FIA_UAU.5.2	IA.2	Self-evident

Requirement	Security Function	Justification
FIA_UAU.7.1	IA.4	Self-evident
FIA_AFL.1.1	IA.5	Self-evident
FIA_AFL.1.2	IA.5	Self-evident
FMT_SMR.1.1	IA.3	Self-evident
FMT_SMR.1.2	IA.3	Self-evident
FAU_GEN.1.1	AUD.1 AUD.2	AUD.1 satisfies FAU_GEN.1.1; AUD.2 identifies where the audit log is stored.
FAU_GEN.1.2	AUD.3	Self-evident
FAU_GEN.2.1	AUD.3	AUD.3 specifically identifies that the user identity shall be stored for each auditable event.
FAU_SAR.1.1	AUD.2	The audit trail is stored as a file on the host operating system for the TOE.
FAU_SAR.1.2	AUD.1 AUD.3 AUD.4	"suitable to interpret" from the SFR is understood to be the functions of AUD.1 and AUD.3 – 4 from a qualitative perspective.
FAU_SAR.2.1	AC.3	Self-evident
FAU_SAR.3.1	AUD.4	Self-evident
FAU_STG.1.1	AC.3	Self-evident
FAU_STG.1.2	AC.3	Prevents access to the audit trail for anyone except and administrative user.
FDP_RIP.2.1	OBJ.1	Self-evident
FDP_ACC.2.1	AC.1 AC.2 AC.5	Together are responsible for defining the applications and functions to which a user is permitted access.
FDP_ACC.2.2	AC.1 – AC.5	Self-evident
FDP_ACF.1.1	AC.2	Self-evident
FDP_ACF.1.2	AC.1 AC.2	Self-evident

Requirement	Security Function	Justification
	AC.5	
FDP_ACF.1.3	-	This is a null requirement, and as such is not *explicitly* met by any SF.
FDP_ACF.1.4	-	This is a null requirement, and as such is not *explicitly* met by any SF.
FMT_MSA.1.1	AC.5	Self-evident
FMT_MTD.1.1	AC.5	Self-evident
FMT_SMF.1.1	AC.4 and AC.5	Self-evident
FTP_ITC.X.1	AC.6	Self-evident
FTP_ITC.X.2	IA.6	In the TLS protocol, the client makes the initial request for a TLS session; the Tarantella Server then authenticates itself to the client.
FTP_ITC.X.3	IA.6	Self-evident
FPT_ITT.1.1	AC.6 AC.7 AC.8	Self-evident
FPT_ITT.3.1	AC.7	Self-evident
FPT_ITT.3.2	AC.8	Self-evident
FCS_COP.1.1	AC.6	Self-evident

Table 7.6 Mapping of Security Functions to Function Requirements

7.3.2 Suitability of the Assurance Measures

Section 6.3 demonstrates that, for each SAR, there is an appropriate assurance measure.

7.4 PP Claims Rationale

This ST does not claim conformance with any PP.

This Page Intentionally Blank