UK IT SECURITY EVALUATION AND
CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P214

TARANTELLA ENTERPRISE 3

**Version 3.40.911 with Tarantella Advanced Security Pack, Version 3.41.211
running on specified platforms**

Issue 1.0

May 2005

UK IT Security Evaluation and Certification Scheme, Certification Body,
CESG, Hubble Road, Cheltenham, GL51 0EX
United Kingdom

**ARRANGEMENT ON THE
RECOGNITION OF COMMON CRITERIA CERTIFICATES
IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY**

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements contained in the certificate and Certification Report are those of the Qualified Certification Body which issued it and of the Evaluation Facility which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Trademarks:

CERTIFICATION STATEMENT

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

Tarantella Enterprise Server 3, Version 3.40.911, with Tarantella Advanced Security Pack, Version 3.41.211, has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL2 for the specified Common Criteria Part 2 extended functionality in the specified environment when running on the platforms specified in Annex A.

Originator	**CESG** Certifier
Approval and Authorisation	**CESG** Technical Manager of the Certification Body UK IT Security Evaluation and Certification Scheme
Date authorised	13 May 2005

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

AIP	Adaptive Internet Protocol (Tarantella)
CC	Common Criteria
CGI	Common Gateway Interface
CLEF	Commercial Evaluation Facility
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HTTPS	Hypertext Transmission Protocol (Secure)
MD5	Message Digest 5
RDP	Remote Desktop Protocol
SFR	Security Functional Requirement
SoF	Strength of Function
SPARC	Scalable Processor Architecture
SSH	Secure Shell
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE Security Functions
UKSP	United Kingdom Scheme Publication
URL	Uniform Resource Locator
VM	Virtual Machine

(This page is intentionally left blank)

REFERENCES

a. Tarantella Enterprise 3 Security Target,
LogicaCMG UK Ltd.,
309.EC200409:40.1, Issue 2.4, 11 April 2005.

b. Common Criteria for Information Technology Security Evaluation,
Part 1, Introduction and General Model,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-001, Version 2.2, January 2004.

c. Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Requirements,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-002, Version 2.2, January 2004.

d. Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Requirements,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-003, Version 2.2, January 2004.

e. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 5.0, July 2002.

f. CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4, April 2003.

g. CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 1.0, October 2003.

h. Common Methodology for Information Technology Security Evaluation,
Evaluation Methodology,
Common Criteria Interpretations Management Board
CEM-2004-01-004, Version 2.2, January 2004.

i. Final Evaluation Technical Report for LFL/T206, Tarantella,
LogicaCMG CLEF,
CLEF.2004097/7.2/1, Issue 1.0, 21 January 2005.

j. Tarantella Enterprise 3, Version 3.4: Installation Guide,
Tarantella Ltd.,
http://www.tarantella.com/support/documentation/enterprise/e3.4/install.html,
7 September 2004.

k. Tarantella Enterprise 3, Version 3.4: Administration Guide,
Tarantella Ltd.,
http://www.tarantella.com/support/documentation/enterprise/e3.4/help/en-us/admintocs/TOC_FUNC_TYPE.html,
29 April 2004.

l. Tarantella Advanced Security Pack Version 3.4 Implementation Guide,
Tarantella Ltd.,
http://www.tarantella.com/support/documentation/enterprise/e3.4/updates/Implementing_tasp.pdf .

m. Tarantella Enterprise 3: Common Criteria Evaluated Configuration Guide,
Tarantella Ltd.,
DART/TTAIN/65/T206 ECG.DOC/1.8, Issue 1.8, April 2005.

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of Tarantella Enterprise 3, Version 3.40.911 with Tarantella Advanced Security Pack Version 3.41.211, to the Sponsor, Tarantella Ltd., and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers are advised to read this report in conjunction with the Security Target [Reference a] which specifies the functional, environmental and assurance evaluation requirements.

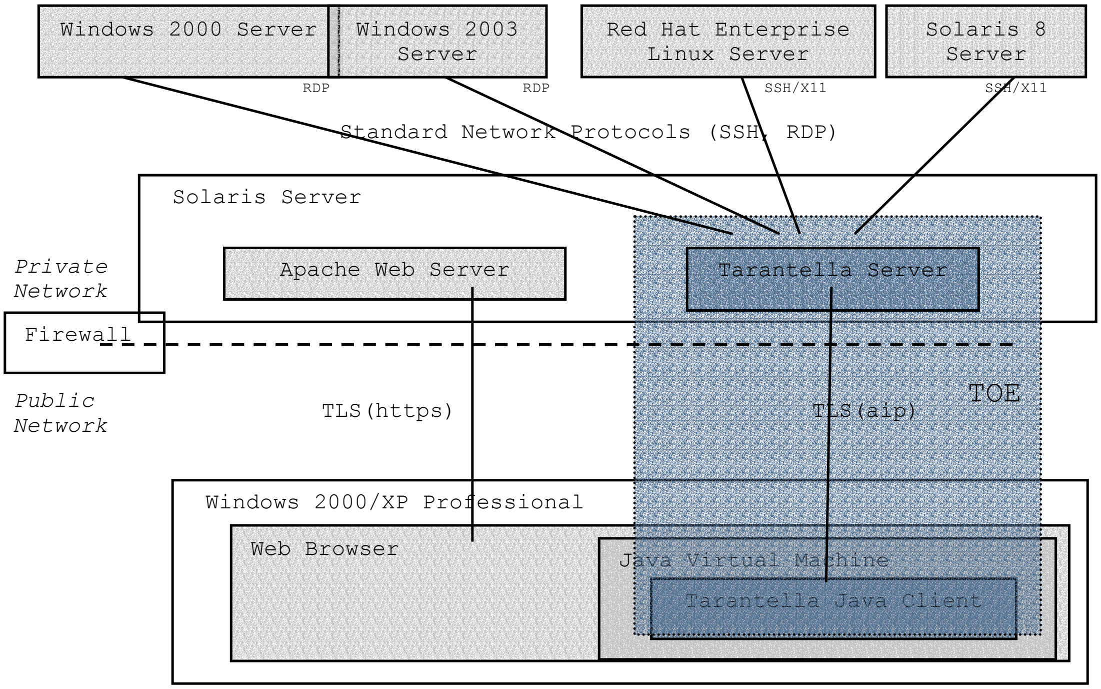
Evaluated Product

3. The version of the product evaluated was:

Tarantella Enterprise 3 Version 3.40.911, with Tarantella Advanced Security Pack Version 3.41.211 and Tarantella '*cgi replacements'* software update.

This product is also described in this report as the Target of Evaluation (TOE). The Developer was Tarantella Ltd.

4. Tarantella Enterprise 3 provides secure, managed, web-based access to server-based applications. It is located between the users, who access it via a Java-enabled web browser, and the server-based applications, which the TOE delivers via a network.



5. Supported back-end Application Servers include Microsoft Windows 2000 and Windows 2003, Red Hat Linux 3.0 and Solaris 8. Users should note that these Application Servers and the communications with them are out of scope of the evaluation.

6. Users login to the Tarantella Server via a web browser and are then presented with a list of applications which they are allowed to run. A single click on an application icon then launches the selected application on its remote server and opens a browser window. The user is then able to interact with the remote application as though it were running locally.

7. 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.

8. The user's experience is one of the following.

- Point the browser at the URL of the Tarantella Server.
- The Tarantella client is downloaded and starts up.
- Login to the Tarantella Server via downloaded client.
- See a list of applications which the user is 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 Tarantella client-server communications are TLS-encrypted through the Tarantella Advanced Security Pack.

9. The administrator uses the Tarantella Object Manager administration tool via a local host machine (either directly attached to the Tarantella Server or from a remote workstation) 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.

10. All application access is managed through the Tarantella Server using the Tarantella Array Manager administration tool. This provides administrator control and knowledge of user access to applications.

11. The evaluated configuration is as illustrated in the diagram above although the firewall shown is out of scope. The product can be used in more complex network environments. These network configurations, which are not certified, may include the firewall shown and an additional firewall between the Tarantella and Application Servers.

12. Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

13. An overview of the TOE's security architecture can be found in Annex B.

TOE Scope

14. The TOE consists of the Tarantella Server software, which resides on its own Solaris 8 server, and the Tarantella Client software, on the user's Windows workstation (either Windows 2000 or Windows XP).

15. The following are excluded from the TOE scope but form part of the TOE Environment:

a. The Operating System and hardware platform supporting the Tarantella Client.

b. Internet Explorer and the Sun Java plug-in on the Tarantella client.

c. The Solaris 8 Operating System, Apache web server and hardware platform on the Tarantella Server.

d. Any optional firewalls, e.g. between the Tarantella Client and the Tarantella Server, or between the Tarantella and the application servers.

e. The application software, Operating Systems and hardware platforms for the Application Servers.

f. Software communications between the Tarantella Server and the Application Servers.

Protection Profile Conformance

16. The Security Target [a] did not claim conformance to any protection profile.

Assurance

17. The Security Target [a] specified the assurance requirements for the evaluation. Predefined Evaluation Assurance Level EAL2 was used. Common Criteria (CC) Part 3 [d] describes the scale of assurance given by EAL1 to EAL7. An overview of CC is given in CC Part 1 [b].

Strength of Function Claims

18. The minimum Strength of Function (SoF) was SoF-Basic. There are no permutational or probabilistic mechanisms in the TOE.

Security Function Policy

19. The TOE has an explicit user access control Security Function Policy, defined in the following Security Functional Requirements (SFRs):

- (user data protection): FDP_ACC.2, FDP_ACF.1
- (security management): FMT_MSA.1

20. See the Security Target [a] for details.

Security Claims

21. The Security Target [a] fully specifies the TOE's security objectives, the threats and Organisational Security Policies which these objectives meet, and SFRs and security functions to elaborate the objectives. Most of the SFRs are taken from CC Part 2 [c]; use of this standard facilitates comparison with other evaluated products.

22. The following explicitly stated SFR extends the CC Part 2 family FTP_ITC, Confidentiality of Exported TOE Security Function (TSF) Data.

a. FTP_ITC.X.1, which requires that the TSF should provide a communication channel between the Tarantella Client and the Tarantella Server.

b. FTP_ITC.X.2, which requires that the TSF should permit the Tarantella Client to initiate communication via this trusted channel.

c. FTP_ITC.X.3, which requires that the TSF should initiate communication via this trusted channel for authentication and other communication.

Evaluation Conduct

23. The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 (UKSP 01) and UKSP 02 [e - g]. The Scheme has established a Certification Body which is managed by CESG on behalf of Her Majesty's Government. As stated on page ii of this Certification Report, the Certification Body is a member of the Common Criteria Recognition Arrangement, and the evaluation was conducted in accordance with the terms of this Arrangement.

24. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [a], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3 [d] and the Common Evaluation Methodology [h].

25. The Certification Body monitored the evaluation which was carried out by the LogicaCMG Commercial Evaluation Facility (CLEF). The evaluation was completed when the CLEF submitted the final Evaluation Technical Report (ETR) [i] to the Certification Body in January 2005. Following the CLEF responses to requests for further information, the Certification Body then produced this Certification Report.

General Points

26. The evaluation addressed the security functionality claimed in the Security Target [a] with reference to the assumed operating environment specified by the Security Target. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and to give due consideration to the recommendations and caveats of this report.

27. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities may be discovered after a certificate has been awarded. This Certification Report reflects the Certification Body's view at the time of certification. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued and, if appropriate, should check with the Vendor to see if any patches exist for the products and whether such patches have been evaluated and certified.

28. The issue of a Certification Report is not an endorsement of a product.

(This page is intentionally left blank)

II. EVALUATION FINDINGS

Introduction

29. The evaluation addressed the requirements specified in the Security Target [a]. The results of this work were reported in the ETR [i] under the CC Part 3 [d] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with the subsequent assurance maintenance and re-evaluation of the TOE.

Delivery

30. The Tarantella Enterprise 3 Base Component should be installed by downloading it from: https://www.tarantella.com/download/predownload.php?product=e3.

The MD5 hash value should be checked after download against the value published on the download pages. This value is:

- 7485816857bb18629b5efa68803f7ba6

31. The Tarantella Enterprise 2 Advanced Security Pack should be installed by downloading it from:
https://www.tarantella.com/download/predownload.php?product=e3.

The MD5 hash value should be checked after download against the value published on the download pages. This value is:

- 23e6579715f99b5c573f1b9082c32393

32. An additional software update, entitled *'cgi replacements'*, should be downloaded from: https://www.tarantella.com/support/updates/e3/bin.605393/

The MD5 hash values should be checked after download against the value published on the download pages. These values are:

• for ttaarchives.cgi.gz	3d59307c00b016e1d263ff484ee14288
• for ttacab.cgi.gz	348b2a28ba4f2d9778afe7612ff47a5f

33. Before loading software as described above users have to be authorized and registered by Tarantella.

34. On receipt of the TOE, the consumer is recommended to check that the evaluated versions of its constituent components have been downloaded, and to check that the security of the TOE has not been compromised in delivery.

35. There are no alternative modes of delivery.

Installation and Guidance Documentation

36. Installation and guidance documentation is provided on-line in the Tarantella Enterprise 3 Installation and Administration Guides [j, k] and the Advanced Security Pack Implementation Guide [l]. All of these documents are available from the Tarantella web site at www.tarantella.com.

37. Further guidance on the evaluated configuration is provided in the Tarantella Enterprise 3 Common Criteria Evaluated Configuration Guide [m]. This is also available from the Tarantella web site, as a link from the Administration Guide [k].

Strength of Function

38. The SoF claim for the TOE was as given above under "Strength of Function Claims". Based on their examination of all the evaluation deliverables, the Evaluators confirmed that there were no probabilistic or permutational mechanisms in the TOE and that the SoF claim of SoF-Basic was therefore upheld.

39. The Phaos and RSA BSAFE cryptographic modules are both validated to FIPS 140-2 level, with validation certificates 337 and 364 respectively. (See http://csrc.nist.gov/cryptval/140-1/140crt/)

40. Developer tests repeated by the Evaluators included some testing of these cryptographic modules installed on the TOE.

Vulnerability Analysis

41. The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

42. The Evaluators found no exploitable vulnerabilities in the TOE.

Independent Testing

43. The Evaluators carried out their independent functional tests and penetration tests at the Developers' site on 20-22 December 2004.

44. The Evaluators made a number of recommendations as a result of their independent functional testing.

45. The TOE allows two users to share the same common name, e.g. two separate users could both be called 'Arthur Smith'. When this occurred there were errors in the logon process for ambiguous users, as the TOE failed to resolve which ambiguous user was trying to gain access. This produced a vulnerability which was countered only by effectively disallowing such ambiguous names. It is recommended that this vulnerability is addressed in the next release of Tarantella, for example by the software itself disallowing the use of ambiguous names.

46. As a result of their independent testing, the Evaluators made some recommendations about minor changes to be incorporated in future versions, for example:

a. Login lockout events should be logged.

b. Documentation should provide a warning that changing a user's Organisational Unit during a webtop session does not take effect at the next login, but affects the current session.

III. EVALUATION OUTCOME

Certification Result

47. After due consideration of the ETR [i], produced by the Evaluators, (as supplemented by further clarifications from the Evaluators,) and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that Tarantella Enterprise 3, Version 3.40.911 with Tarantella Advanced Security Pack, Version 3.41.211, meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL2 for the specified Common Criteria Part 2 extended functionality, in the specified environment, when running on the platforms specified in Annex A.

48. The minimum Strength of Function was SoF-basic. The TOE itself contains no probabilistic or permutational mechanisms and so a minimum SoF claim was not relevant.

Recommendations

49. Prospective consumers of Tarantella Enterprise 3 Version 3.40.911 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [a]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

50. Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under ‘TOE Scope’ and ‘Evaluation Findings’.

51. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration [j - m].

52. The assurance of security provided by this report applies only to the TOE. Consumers should also consider the security of the environment. For example, the Operating Systems in the environment should be securely configured and should have security patches applied where appropriate.

53. The above ‘Evaluation Findings’ include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

(This page is intentionally left blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE consists of:

- Tarantella Enterprise 3 Base Component Version 3.40.911.
- Tarantella Enterprise 3 Advanced Security Pack Version 3.41.211.
- Tarantella 'cgi replacements' software update.

2. Tarantella Enterprise 3 Base Component consists of the following:

- Tarantella Enterprise 3 Server.
- Tarantella Enterprise 3 Java Client.
- Tarantella Enterprise 3 Administration Tools (Tarantella Object Manager; Tarantella Array Manager and Tarantella Command Line Interfaces).

3. The TOE can only be delivered from the Tarantella internet web site as described in Section II under ‘Delivery’.

TOE Documentation

4. The supporting guidance documents evaluated were:

- Tarantella Enterprise 3 Installation Guide [j]
- Tarantella Enterprise 3 Administration Guide [k]
- Tarantella Advanced Security Pack Implementation Guide [l].
- Tarantella Enterprise 3 Common Criteria Evaluated Configuration Guide [m].

5. Guidance documentation [j - m] is only available from the Tarantella internet web site as described in Section II under ‘Installation and Guidance Documentation’.

TOE Configuration

6. Further guidance on the evaluated configuration is provided in the Tarantella Enterprise 3 Common Criteria Evaluated Configuration Guide [m].

Environmental Configuration

7. The Tarantella Client software runs on a standard PC with at least 32 Mbytes memory, using either Windows 2000 Professional or Windows XP Professional, together with Internet Explorer 6 Service Pack 1 and Sun Java Virtual Machine 1.4.2.

8. The Tarantella Server software runs on a Sun compatible server with a SPARC processor and at least 256 Mbytes memory, using Solaris 8 02/02 with Apache web server.

9. Consumers of Tarantella Enterprise 3 should note the need to configure securely the software in the environment, for example the Operating Systems and web browser software, and should check for the existence of security patches to this software.

10. Application Servers can be any hardware platforms supporting one of the following Operating Systems:

- Windows Server (Windows 2000 or Windows 2003), configured as a Terminal Server, supporting RDP.
- Red Hat Linux Enterprise 3 Server, configured to support SSH2 and X11 protocols.
- Solaris 8 Server, configured to support SSH2 and X11 protocols.

11. Firewalls should be used to contribute to network security where communications between the Tarantella Client and the Tarantella Server, or between the Tarantella Server and Application Servers, use potentially hostile networks.

12. When a firewall is used, between the Tarantella Client and the Tarantella Server, it should be configured so that all ports are blocked except for a two-way TCP connection for the Tarantella Server on port 443.

Environmental Test Configuration

13. The following configuration was used for testing.

a. The Tarantella Client software installed on two separate platforms in order to test Windows XP Pro and Windows 2000 Pro. Most Evaluator tests were repeated on each platform.

i. One Client was a Toshiba Tecra laptop with an Intel Pentium III, 366 MHz, 128 MB RAM, 13.1 GB hard disk and a 10 Mbps Ethernet card, running Windows 2000 Service Pack 4 with Internet Explorer 6, Service Pack 1, and Sun Java Virtual Machine 1.4.2.

ii. The other Client was a Compaq Armada M700 laptop with an Intel Pentium III, 650 MHz, 256 MB RAM, 12 GB hard disk and a 10 Mbps Ethernet card, running Windows XP, Service Pack 2 with Internet Explorer 6, Service Pack 1, and Sun Java Virtual Machine 1.4.2.

b. Tarantella Server software installed on a Sun Fire 280R Server with 1.2 GHz Ultra SPARC III and 2 GBytes memory, running Solaris 8 02/02, with Apache web server 1.3.

14. For the test configuration a Cisco PIX 501 firewall was used between the Tarantella Client and the Tarantella Server.

15. In the test configuration, four Application Servers (connected to the Tarantella server by a network hub) were used, with the following Operating Systems:

- Windows 2000.
- Windows 2003.
- Red Hat Enterprise Linux.
- Solaris 8 Server.

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. This annex gives an overview of the main product architectural features that are relevant to the security of the TOE. Other details of the scope of evaluation are given in the main body of the report and in Annex A.

Architectural Features

2. For an introduction to the TOE architectural features see Section I under 'Evaluated Product'.

3. The TOE relies on services provided by the underlying Operating Systems, for Identification and Authentication, as identified in the Security Target [a].

Design Subsystems

4. The design subsystems are as follows.

a. Tarantella Client software, handling traffic between the Tarantella Client and the Tarantella Server;

b. JServer, providing identification and authentication;

c. The Datastore, holding configuration information for the TOE and its users;

d. TLS Daemon, handling traffic sent between the Tarantella server and client servers, and encryption and decryption;

e. Admin Tools, for creating and modifying Tarantella's user accounts;

f. Protocol Engine Manager (*);

g. Protocol Engines (*);

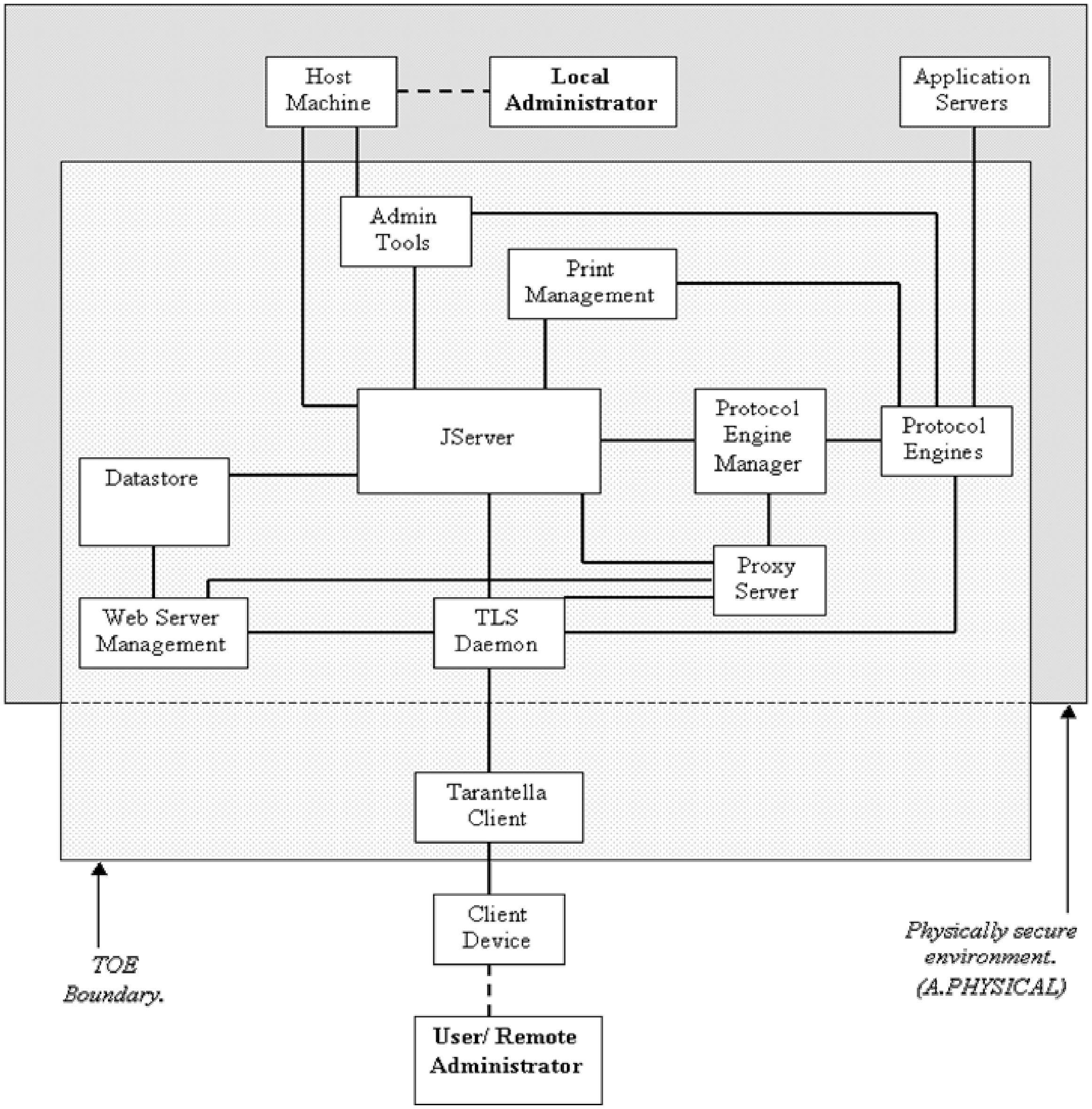
h. Web Server Management (*);

i. Print Management (*); and

j. The Proxy Server (*).

5. Only the first five of these subsystems provide TSF enforcing functionality. Those marked with an asterisk (*) do not.

6. Communications between the subsystems and externally are illustrated in the following diagram.



7. Local administration works directly on the Tarantella Server platform. Remote administration uses the Tarantella connection to enable administration from a client machine.

Platform Dependencies

8. The TOE has no hardware or firmware dependencies and relies on the environmental Operating Systems for all communication with hardware platforms.

9. The TOE relies on the Operating System and hardware platform of its environment for:

a. external (server based Unix) authentication;

b. protection of audit records and other data;

c. import of keys;

d. reliable timestamps for audit records; and

e. network communication between parts of the TOE.

TSF Interfaces

10. The external interfaces to the TOE are identified as:

a. The Graphical User Interface (GUI) for User Login, providing user authentication;

b. The Webtop GUI, used to launch applications;

c. The Array Manager GUI for administrators only, to manage the TOE configuration;

d. The Object Manager, for administrators only, to manage the TOE configuration;

e. The Command Line Interface, for administrators only, to manage the TOE, and

f. The Network Interface - between the Tarantella Client and Tarantella Server, and also between the Tarantella Server and Application Servers, using RDP, SSH2, X11 and TLS protocols.

(This page is intentionally left blank)

ANNEX C: PRODUCT TESTING

IT Product Testing

1. The Developers' tests covered all the security functions but one security function was not fully exercised. The Evaluators devised independent tests to cover each security function and to fully test the one not fully covered by Developer testing. The Evaluators also successfully repeated approximately 50% of the initial Developers' tests.

2. The TOE subsystems and TSF Interfaces are listed above in Annex B.

3. Developer testing covered all subsystems of the TOE and all TSF Interfaces. Similarly, the Evaluators' independent functional tests also covered all subsystems and all TSF Interfaces. Both local and remote administration methods were tested.

4. Penetration tests covered the areas of Identification and Authentication; Audit and Accountability and Access Control.

(This page is intentionally left blank)