UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P225

Hewlett-Packard HP-UX
Version 11.23 (11i Version 2)
running on HP 9000 or HP Integrity platforms

Issue 1.0

May 2006

UK Certification Body,
CESG, Hubble Road,
Cheltenham, GL51 0EX
United Kingdom

CERTIFICATION STATEMENT

The product detailed below has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the specified Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.	
Sponsor	**Hewlett-Packard Company**
Product and Version	**HP-UX 11.23 (11i Version 2)**
Description	HP-UX is Hewlett-Packard's implementation of the UNIX Operating System
CC Part 2	**Conformant**
CC Part 3	**Extended**
EAL	**EAL4** augmented by ALC_FLR.3, Systematic Flaw Remediation
Protection Profiles	**CAPP and RBAC**
CLEF	**LogicaCMG**
Certifier	**CESG**
Date authorised	25 May 2006

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 ([a] - [c]). The Scheme has established a Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [d], 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 [j], the Common Evaluation Methodology (CEM) [k], and relevant Interpretations.

The issue of a Certification Report is a confirmation that the evaluation process has been carried out properly and that no exploitable vulnerabilities have been found. It is not an endorsement of the product.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of HP-UX 11.23 (11i Version 2) to the Sponsor, the Hewlett-Packard Company, 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 [d], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The version of the product evaluated was:
HP-UX 11.23 (11i Version 2)
also referred to in this Report as **HP-UX 11i v2**.

4. The Developer was the Hewlett-Packard Company.

5. HP-UX 11i v2 is an Operating System based on UNIX. The evaluated product may execute on a single HP 9000 (PA-RISC) Server or HP Integrity Server, which may be connected to other CAPP compliant Servers forming a local distributed system.

6. The evaluated configuration of this product is described in this report as the Target of Evaluation (TOE). Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III 'Evaluated Configuration'.

7. An overview of the product and its security architecture can be found in Chapter IV 'Product Security Architecture'.

Protection Profile Conformance

8. **The Security Target [d] is certified as achieving conformance to the following protection profiles:**

Controlled Access Protection Profile (CAPP) [e].
Role Based Access Control Protection Profile (RBAC PP) [f].

9. The Security Target [d] also includes objectives and security functions additional to those of the protection profiles.

Security Claims

10. The Security Target [d] fully specifies the TOE's security objectives, the Organisational Security Policies (OSPs) which these objectives support and the Security Functional Requirements (SFRs) and security functions to elaborate the

objectives. All of the SFRs are taken from CC Part 2 [i]. Use of this standard facilitates comparison with other evaluated products.

11. The Security Target [d] makes security functionality claims for the TSF grouped under the following categories:

- identification and authentication
- access control
- audit
- object reuse
- protection functions.

Strength of Function Claims

12. **The minimum Strength of Function (SoF) was SoF-Medium**. This was claimed for the password checking mechanism. **The Certification Body has determined that these claims were met.**

13. The Security Target [d] states that the claimed minimum SoF for the password-checking mechanism, SoF-medium, is consistent with the CAPP Security Functional Requirement FIA_SOS.1 as justified in CAPP Section 7.5 [e].

14. The CAPP security functional requirement FIA_SOS.1 states that the password-checking mechanism should meet the following.

a. For each attempt to use the authentication mechanism, the probability that a random attempt will succeed is less than one in 1,000,000.

b. For multiple attempts to use the authentication mechanism during a one minute period, the probability that a random attempt during that minute will succeed is less than one in 100,000.

c. Any feedback given during an attempt to use the authentication mechanism will not reduce the probability below the above metrics.

15. In addition, the Security Target states that the product implements a modified one-way DES algorithm to satisfy the password encryption algorithm specified. This cryptographic mechanism is publicly known and as such it is the policy of the national authority for cryptographic mechanisms, CESG, not to comment on its appropriateness or strength.

Evaluation Conduct

16. The TOE Security Functions and security environment, together with much of the supporting evaluation deliverables, remained mostly unchanged from an earlier version of HP-UX 11i, which had previously been certified by the UK IT Security Evaluation and Certification Scheme to the CC EAL4 assurance level [g]. **For the evaluation of HP-UX 11i v2, the Evaluators addressed every CEM [k] EAL4 work unit but made some use of the earlier HP-UX 11i evaluation results where appropriate.**

17. The Certification Body monitored the evaluation which was carried out by the LogicaCMG Commercial Evaluation Facility. The evaluation addressed the

requirements specified in the Security Target [d]. The results of this work, completed in April 2006, were reported in the Evaluation Technical Report [l].

Conclusions and Recommendations

18. The conclusions of the Certification Body are summarized in the Certification Statement on page 2.

19. **Prospective consumers of HP-UX 11i v2 should understand the specific scope of the certification by reading this report in conjunction with the Security Target** [d].The TOE should be used in accordance with the environmental assumptions specified in the Security Target. 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.

20. **This Certification Report is only valid for the evaluated TOE**. This is specified in Chapter III 'Evaluated Configuration'.

21. **The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration**. Chapter II 'Product Security Guidance' below includes a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

22. **Prospective consumers and authorised administrators should be aware of certain issues arising from the use, on the TOE, of POSIX-compliant utilities that do not handle all security attributes.** This arises from the fact that the TOE is a POSIX-compliant UNIX operating system with added security features. As noted in [m], section 5.9, whilst a large number of POSIX-compliant programs will work adequately, legacy programs may be unaware of the security features in the TOE and, so, may harm the configuration of the system. See also [n] for more details.

23. **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 these patches have further assurance. The installation of patches for security vulnerabilities, whether or not they have further assurance, should improve the security of the product

II. PRODUCT SECURITY GUIDANCE

Introduction

24. The following sections note considerations that are of particular relevance to purchasers of the product.

Delivery

25. **On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery**.

26. Secure delivery of the TOE is described in the Delivery Procedures [q] available from HP, which describe the process of releasing the TOE to consumers.

27. For the evaluated product, customers should contact common_criteria_inquiries @cup.hp.com. The relevant software discs are then despatched to the customer, securely shrink-wrapped, by a trusted courier. The customer receives a packing list which includes the customer's purchase order number, an internal HP order number and a list of boxes with their contents. Each box is sealed with a label which includes both order numbers, the box number and its contents.

28. Users should note that delivery procedures will change in August 2006. Customers will then use similar standard HP delivery procedures, specifying option A54 of product B8483AA for the evaluated version. **The Evaluators have not been able to test the new procedures for delivery.**

29. Patches may be sent out to consumers using the trusted delivery procedures or they may be downloaded from the HP support website. The website requires a user ID and password. Note, however, that there is no inherent security in the download of patches from the HP support website and consumers are recommended to request delivery of the patches from HP using the trusted procedure described above for delivery of the operating system.

Installation and Guidance Documentation

30. The guidance documents evaluated were:

- Common Criteria HP-UX 11i v2 Evaluated Configuration Guide [m]
- Managing Systems and Workgroups: A Guide for HP-UX System Administrators [n].
- HP-UX 11i Security Containment Administrator's Guide [o].
- Software Distributor Administration Guide [p].
- Trusted Delivery [q]
- HP-UX 11i Installation and Update Guide [r]
- Using HP-UX [s]

31. Secure installation, generation and startup of the TOE are described in [m] - [s].

32. The Evaluated Configuration Guide [m] should be read first, as it details the steps that must be followed to install the TOE in its evaluated configuration. The Evaluated Configuration Guide references the Installation and Update Guide [r] and the Administrator Guide [n], as appropriate, and a number of other minor documents (including Release Notes files to be found on the product's delivery discs).

33. When the installation of the TOE is complete, the *man* Pages (which provide on-line help information) can be accessed.

Flaw Remediation

34. In addition to the EAL4 evaluation, the evaluators also assessed the Common Criteria Part 3 assurance component ALC_FLR.3, Systematic Flaw Remediation, and found that the TOE met this requirement.

35. The Evaluated Configuration Guide [m] includes instructions to users to check for reported flaws at the HP IT Resource Center (ITRC) site. It also describes a free alerting service which users can subscribe to.

36. As a result of their Flaw Remediation process, HP may include additional security patches to the delivery process for the TOE, including them on the delivered CDs and/or noting them in an updated Evaluated Configuration Guide.

III. EVALUATED CONFIGURATION

TOE Identification

37. The TOE is uniquely identified as:
HP-UX Version 11.23 (11i Version 2) with a number of patches identified in the Evaluated Configuration Guide [m].

38. The DVD for the software is identified as **HP-UX 11i Version 2, Mission Critical Operating Environment, Core OS Install and Recovery DVD, Version B.11.23, May 2005, Part No. B8483-60040**.

TOE Documentation

39. The relevant guidance documentation for the evaluated configuration is identified above under 'Installation and Guidance Documentation'.

40. Two additional discs are supplied with the software DVD. One is identified as **HP-UX 11i Version 2, HP Instant Information Documentation Library DVD, May 2005, Part No. 50726-10497**.

41. The other is a Common Criteria supplemental disc specific to this evaluation, containing the Security Target, The Evaluated Configuration Guide, other documentation (including Release Notes) and incremental patches[1]. This is identified as **HP-UX 11i v2 May 2005 Common Criteria Supplementary CD, Version 1.0, April 2006, Part No. 5013-2684.**

TOE Scope

42. The Evaluated Configuration Guide [m] provides details of the evaluated configuration of HP-UX 11i v2. In summary.

a. The evaluated product may execute on a single HP 9000 (PA-RISC) Server or HP Integrity Server, which may be connected to other CAPP compliant Servers forming a local distributed system. (For a fuller discussion of the consideration given to hardware platforms see 'Platform Issues' below.)

b. The TOE supports user interaction via any of the supported Shells including the POSIX, Bourne, C and Korn Shells.

c. The TOE supports the HFS and JFS file systems but excludes Online JFS.

d. The TOE includes Pluggable Authentication Modules (PAM) with default configuration for authentication consisting of user identity and password.

e. The TOE executes with CDE and X-Windows disabled and excludes the use of a restricted configuration of the System Administration Manager (SAM).

f. The TOE includes socket based network functions and the following network applications - ftp, rexec, rlogin and telnet.

---

[1] Note that the formal production of this final CD will mark the change in delivery processes described above in Chapter II, under 'Delivery'

43. The following are excluded from the evaluation.
- The Online JFS file system.
- X-Windows
- Network applications other than those listed above (e.g. NFS and NIS).

TOE Configuration

44. The TOE should be configured in accordance with the Evaluated Configuration Guide [m] and the guidance documents.

Environmental Requirements

45. The Security Target [d] includes a number of assumptions about the environment. These include trusted authenticated users; competent security administration; and practices and policies to support security.

46. Details of the TOE's environmental configuration are summarised above under 'TOE Scope'.

Test Configuration

47. The Developers performed their testing of the TOE on the following hardware platforms:

a. Hewlett-Packard HP 9000 server rp3440 (A7137A):
- 4 PA 8900, 800 MHz CPU
- 4 GByte RAM
- 3 36 GByte hard disks.

b. Hewlett-Packard HP 9000 server rp7420 (AB206A):
- 8 PA 8800, 900 MHz CPU
- 8 GByte RAM
- 4 73 GByte hard disks.

c. Hewlett-Packard HP Integrity server rx1620 (AB431A):
- 1 Itanium 2, 1.6 GHz CPU
- 1 GByte RAM
- 2 36GB hard disks.

d. Hewlett-Packard HP Integrity server rx2620 (AB331A):
- 2 Itanium 2, 1.6 GHz CPU
- 2 GByte RAM
- 3 36GB hard disks.

e. Hewlett-Packard HP Integrity server rx4640 (AB370A):
- 8 Itanium 2, 1.1 GHz CPU
- 8 GByte RAM
- 2 73 GByte hard disks.

48. The Evaluators conducted their testing on the hardware platforms identified above. During the Evaluators' independent testing, the above machines were networked to

allow testing of the network commands included within the TOE. **All tests were repeated, successfully, on all the platforms listed above.**

49. In addition, as discussed below under 'Platform Issues', the evaluation results were determined, through analysis, to hold for other HP 9000 and HP Integrity servers.

50. The servers for which the evaluation results hold are as follows.

- HP 9000 series - rp3410; rp3440; rp4410; rp4440; rp7420; rp8420 and superdome.
- HP Integrity series - rx1600; rx1620; rx2600; rx2620; rx4640; rx5670; rx7620; rx7640; rx8620; rx8640; cx2600; zc2000; zx6000; BL60p and superdome.

IV. PRODUCT SECURITY ARCHITECTURE

51. This Chapter gives an overview of the main product architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration'.

Product Description and Architecture

52. The product may execute on a single HP Server or be connected to other Servers also running under CAPP compliant Operating Systems forming a local distributed system.

53. The product incorporates network functions but contains no network specific security requirements. Networking is covered only to the extent to which the product can be considered to be part of a centrally managed system that meets a common set of security requirements.

54. The main security features of the product are:

- user identification and authentication
- discretionary access control (DAC), including access control lists
- auditing
- object reuse protection
- Role Based Access Control.

Identification and Authentication

55. All users of the product are authenticated and held accountable for their security related actions. Each user is uniquely identified by the product. The product records security related events and the user associated with the event.

56. The product supports an ordinary *user* role and an *authorized administrator* (administrative) role. An authorized administrator has 'root privilege' and is not constrained by the product's security policies.

57. The product allows an authorized administrator to associate individual users with a privileged group, thus permitting a process acting on the user's behalf to change the ownership of files.

58. The authentication features are supported by constraints on user-generation of passwords and an encryption mechanism.

Discretionary Access Control

59. All subjects are associated with an authenticated user identity, and all named objects are associated with identity-based protection attributes. These are used as the basis of DAC decisions, which control the access of subjects to objects.

60. The product implements a DAC policy, which provides both the traditional UNIX 'owner', 'group', 'other' access mode permissions and a more granular Access Control List (ACL) mechanism, controlled by the object's owner.

61. The product implements 2 independent ACL mechanisms.
- HFS ACLs for the HFS File System.
- JFS ACLs for the JFS File System.

62. DAC is supported by object reuse mechanisms to ensure that information is not inadvertently transferred between subjects when objects are re-allocated.

Auditing

63. The product is capable of collecting audit records for all security relevant events that occur. An authorized administrator may select the users and events for which audit data is collected from time to time.

64. Audit records may be viewed by an authorized administrator selectively for any period on the basis of criteria such as user name, event type and outcome.

65. Facilities are provided to enable the authorized administrator to manage audit log files and to ensure that audit data is retained during abnormal conditions. Note that audit records are buffered in memory before they are written to disk. In these cases it is likely that some of these records will be lost if the operation of the TOE is interrupted by hardware or power failures.

Object Reuse Protection

66. Memory is allocated, managed, and access controlled, by a multitude of mechanisms, which ensure, for example, that when a page of memory is allocated to a process, only that process, or others that may have authorized access to that memory, can access that memory. Also, when memory is returned and made available for subsequent allocation, that page of memory is zeroed prior to subsequent allocation, to ensure no other process may access residual information contained therein as a result of its use by another process.

Role Based Access Control

67. In addition to the standard access control mechanisms, HP-UX 11i v2 also provides a Role Based Access (RBAC) mechanism as an alternative to the all-or-nothing security model of traditional root user-based systems. With RBAC, an authorized administrator can assign certain roles to non-root users or groups. Each role has certain authorizations composed of an operation and object. Non-root user can then execute commands or applications with elevated privileges that would otherwise be impossible. RBAC is a mechanism that maps users to certain permitted operations.

68. The HP-UX 11.11i v2 system grants permissions to the authorized administrator for all operations, and denies permissions to non-root users on certain operations. This

notion of the privilege checking is simple. But it is difficult to distribute the administrative responsibilities among a group of administrators, as they all need to have the access to the root account to perform any administrative action. For further details see the RBAC Protection Profile [f].

Kernel Subsystems

69. The entire kernel software executes in (hardware/privileged) kernel mode. This allows the kernel to execute privileged hardware instructions and perform low-level I/O. The kernel interface is via instruction trap. User/unprivileged processes call the trap instruction as an interface. There is no separate process that represents the kernel; rather, through the trap instruction, kernel functions are available to every process on the system.

70. The kernel software is a collection of distinct logical subsystems, as follows.

a. Memory Management - provides for access, allocation, deallocation, and control of all memory, for all processes, both kernel and non-kernel, within the system. Interfaces with the hardware for address translation, enable memory sizes far in excess of actual hardware, for all processes. Further, this subsystem tracks all address space allocations to all processes, and prevents the unintended sharing of memory between processes, thereby maintaining address space integrity.

b. Process Management - initiates processes, allocates and deallocates system resources, tracks and manages all processes within the system from point of initiation to final termination (for both kernel, and non-kernel processes).

c. File System and Device Input/Output - provides for the creation, access, and manipulation of file system objects by other processes, and maintains device independence for end user applications. This component provides the interface for low-level device I/O drivers and other processes.

d. Inter Process Communications (IPC) Mechanisms - facilitate the synchronization of processes or events, and the sharing of information, between processes for both kernel and non-kernel processes.

e. Kernel Audit Support - creates and writes Audit records for each of the user selected events and system calls to provide a complete audit trail of user space processes and services of the kernel. A privileged application may also specifically request the kernel to generate a high-level audit record on its behalf.

f. Access Mediation - enforces security policy for DAC to file system objects (FSOs). Functionally, it determines the access rights of the requestor to FSOs, and compares the associated access rights to the security policy of the system, and/or as defined in ACLs, and enforces that policy, for each request.

71. All of the above subsystems provide the interface to the TCB hardware for all processes and objects for the definition and enforcement of the security policy, thereby ensuring system security.

Non-kernel Subsystems

72. The non-kernel TCB contains executable and non-executable components. All executable components in the non-kernel TCB are trusted programs that run in user mode, which prevents them from executing privileged hardware instructions. Note that all non-kernel TCB components have discretionary access set to prevent unauthorized modification.

73. Non-kernel TCB trusted programs consist of specific function-related code combined with common routines found in the system libraries. Although many of these libraries are dynamically linked at execution time, the locations of these libraries are specified by HP at compile time. These libraries are stored in files and memory that cannot be modified by untrusted users.

74. The non-kernel TCB consists of a number of functions that support the operation of the system. The interface, just as any untrusted process, to the TCB, for protected services, is via an instruction trap. The functions are included as a part of the TCB because their operation supports the kernel TCB, and are necessary for administration of the system. The components of the non-kernel TCB are summarized as follows.

a. Audit programs and functions - enable the auditing of processes and events, to a granularity of an individual user, of security relevant actions requested, or taken by the process.

b. System Call Libraries, a set of files containing the executable system calls and service routines invoked by the kernel TCB for accomplishing a trusted function on behalf of an untrusted process.

c. TCB (Trusted Computing Base) Databases, sets of files operated upon, and/or used by the kernel, and non-kernel TCB for the enforcement of the security policy, and administration of the TCB.

d. Binary Libraries - containing the executable files for commands and user initiated actions

e. Trusted Processes, support processes that provide an interface to call on components of the kernel TCB, or allow for modification of user or untrusted process access rights.

f. Trusted Commands - may be initiated by untrusted users, or processes, that are trusted to restrict initiation of the command to those entities that are authorized to do so.

g. Batch Processing Programs - facilities that schedule the initiation and execution of programs at a future date.

h. Role Based Access Control **-** an alternative to the all-or-nothing security model of traditional root user-based systems. With RBAC, an administrator can assign certain roles to non-root users or UNIX groups. Each role has certain authorizations composed of an operation and object.

i. Aries Binary Translator **-** Software which emulates execution of PA-RISC applications on Itanium 2 systems.

j. System Administration Manager - facilitates the definition, maintenance, control, and implementation of the desired security policies to ensure system integrity of the trusted system. Through this subsystem, all access to system resources by all potential users, privileges associated therewith, as well as audit trails, are defined and maintained in SAM's respective databases for use and interface by the foregoing components.

75. The non-kernel TCB also contains security databases, file system objects, and trusted libraries whose access is limited to specific users or groups.

Hardware and Firmware Dependencies

76. The TOE relies on the correct operation of processor mode and memory separation mechanisms to ensure system security.

Product Interfaces

77. The product has a large number of external interfaces with users, with the hardware and with other software. These can be considered in groups as follows.

- User Commands.
- Systems Administration Commands.
- System Calls.
- Library Functions.
- File Formats.

78. There are also internal interfaces between kernel and non-kernel software.

V. PRODUCT TESTING

IT Product Testing

79. Developer testing covered all commands, all system calls, all libraries and all subsystems. They also covered all TOE Security Functions and all external TSF interfaces. Evaluators applied some sampling to their checks on Developer testing.

80. The Evaluators performed independent functional testing on the TOE at Cupertino in California in March 2006, to confirm that it operates as specified. This was based in part on tests devised for the evaluation of HP-UX 11.11 (11i v1) [g] with additional tests which included RBAC. Each TSF was covered by at least one test.

81. The Evaluators then performed penetration testing which confirmed the SoF claimed in the Security Target [d] for the password checking mechanism. The penetration testing also confirmed that all identified potential vulnerabilities in the TOE have been addressed, i.e. that the TOE in its intended environment has no exploitable vulnerabilities.

Vulnerability Analysis

82. The Evaluators' vulnerability analysis, which preceded penetration testing, was based on both public domain sources and the visibility of the TOE given by the evaluation process.

Platform Issues

83. The TOE was tested on the hardware platforms specified above under 'Test Configuration', with each test being performed on a range of platforms.

84. In addition, the Evaluators confirmed their agreement with the Developer's Multi-platform Rationale [t] that the results of the evaluation would be applicable to other hardware platforms. As a result of their examination of this rationale, the Evaluators considered the evaluation outcome should apply to all of the additional platforms identified above under 'Test Configuration'.

85. All of the platforms identified in the Developer's Multi-platform Rationale [t] are of two types based on

- the HP 9000 PA-RISC (Precision Architecture - Reduced Instruction Set Computer) architecture version 2.0, and
- HP's Integrity (Itanium 2) architecture.

86. HP-UX 11i v2 source code is structured to permit common source to be used on all supported platforms (both HP 9000 and HP Integrity). The few exceptions to this rule apply to the lowest level machine dependent kernel code.

87. The hardware in the HP 9000 and HP Integrity platforms varies according to the processor version, processor speed, number of processors, amount of memory, I/O

expandability, I/O buses and types of I/O adapters as allowed by the PA-RISC and Itanium 2 architectures. The Developer's Multi-platform Rationale discusses each of these hardware variations in the context of the assurance requirements and provides justification that none of the variations affect the evaluation results.

VI. REFERENCES

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

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

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

[d] HP-UX Version 11i v2 Security Target against the Controlled Access Protection Profile and the RBAC Protection Profile,
Hewlett-Packard Company,
HP-UX 11i v2 ST, Issue 2.0, 15 May 2006.

[e] Controlled Access Protection Profile,
National Security Agency,
Version 1.d, 8 October 1999.

[f] Role Based Access Control Protection Profile,
National Institute of Standards and Testing,
Version 1.0, 30 July 1998.

[g] Common Criteria Certification Report: Hewlett-Packard HP-UX 11i, Version 11.11,
UK IT Security Evaluation and Certification Scheme,
P176, Issue 1.0, February 2003.

[h] Common Criteria for Information Technology Security Evaluation,
Part 1, Introduction and General Model,
Common Criteria Interpretations Management Board,
CCIMB-2005-08-001, Version 2.3, August 2005.

[i] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Requirements,
Common Criteria Interpretations Management Board,
CCIMB-2005-08-002, Version 2.3, August 2005.

[j] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Requirements,
Common Criteria Interpretations Management Board,
CCIMB-2005-08-003, Version 2.3, August 2005.

[k] Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Evaluation Methodology Editorial Board,
CCIMB-2005-08-004, Version 2.3, August 2005.

[l] Evaluation Technical Report, HP-UX 11i Version 2,
LogicaCMG CLEF,
310.EC201717:30.1, Issue 1.0, 24 April 2006.

[m] Common Criteria HP-UX 11i v2 Evaluated Configuration Guide,
Hewlett-Packard Company,
Version 2.0, 15 May 2006.

[n] Managing Systems and Workgroups: A Guide for HP-UX System Administrators,
Hewlett-Packard Company,
5990-8172, E0904, Edition 7, September 2004,

[o] HP-UX 11i Security Containment Administrator's Guide, HP-UX Servers and Workstations, HP-UX 11i v2,
Hewlett-Packard Company,
5991-1821 E0605, May 2005.

[p] Software Distributor Administration Guide for HP-UX 11i v2,
Hewlett-Packard Company,
B2355-90789, September 2003.

[q] Trusted Delivery,
Hewlett-Packard Company,
Version 2.0, 8 August 1996.

[r] HP-UX 11i v2 Installation and Update Guide,
Hewlett-Packard Company,
5991-0792, Edition 4, May 2005.

[s] Using HP-UX,
Hewlett-Packard Company,
B2355-90164, Edition 3, September 1997.

[t] Multi-Platform Rationale HP-UX 11i v2 Common Criteria,
Hewlett-Packard Company,
HPUX11iv2CC-TN-01, Issue 5.2, 21 April 2006.

VII. ABBREVIATIONS

This list does not include well known IT terms such as LAN, GUI, PC, HTML, ... or standard Common Criteria abbreviations such as TOE, TSF, ... (See Common Criteria Part 1 [h], Section 2.3)

ACL	Access Control List
CAPP	Controlled Access Protection Profile
CDE	Common Desktop Environment
DAC	Discretionary Access Control
FSO	File System Object
HFS	High-speed File System
HP	Hewlett-Packard
ITRC	IT Resource Center
JFS	Journalled File System
NFS	Network File System
NIS	Network Information Service
PAM	Pluggable Authentication Module
PA-RISC	Precision Architecture - Reduced Instruction Set Computer
RBAC	Role Based Access Control
SAM	System Administration Manager
TCB	Trusted Computing Base
VxFS	VERITAS File System (used in some HP documentation but synonymous with JFS)