Security Target B1/EST-X

Version 1.1

Table of Contents

1 ST Introduction

1.1 ST Identification

Title: B1/EST-X Security Target

Keywords: AIX, B1 system, mandatory and discretionary access control

1.2 ST Overview

This document is the Security Target for the evaluation of the Bull B1/EST-X system, Version 2.0. The TOE is a general purpose multi-user, multi-level operating system fulfilling functional requirements of [ITSEC] F-B1 and assurance requirements of EAL4. The following security functionality is provided:

- Mandatory access control
- Discretionary access control
- Identification and authentication (I&A)
- Audit
- Data interchange (import/export)

The B1/EST-X product contains additional features over and above the claims being made and evaluated in this document. These include TCP/IP based communications facilities.

The evaluation is to be performed in accordance with the Common Criteria V 2.0 for computer security evaluation as described in reference [CC20].

The contents of the Security Target follows the requirements as described in the Common Criteria [CC20].

1.3 CC conformance

The security functionality provided by the TOE is identical to the ITSEC functionality class F-B1 as described in [ITSEC].

The TOE reaches the assurance level CC EAL4 augmented with ALC_FLR.2 and a minimum claimed strength of function of high.

2 TOE Description

2.1 Parts of the TOE

The TOE consists of the Bull B1/EST-X system, Version 2.0.1.0.

The Target of Evaluation consists of software and documentation, summarized in the following table:

Nr	Type	Identifier	Form of Delivery
1	SW	Bull B1/EST-X system, Version 2.0.1.0	CD-ROM
2	DOC	Software Release Bulletin for 2.0.1.0, October 5, 1998	Paper

Table 1: Deliverables of the TOE

The TOE is installed on top of AIX 4.3.1. On AIX the TCB option needs to be activated and the PTFs U455989.ptf, U456045.ptf and U456165.ptf need to be applied to the system.

Supported Platforms:

B1/EST-X is submitted for evaluation on Bull Escala RL 470 and IBM S-70 with RS64 processors, and IBM F-50 and Bull Escala T with PowerPC604 processors: the F-50 and Escala T (with 2 up to 4 PowerPC604 processors, PCI bus) have similar architecture but different hardware, the Escala RL470 is the name given to S-70 model which is sold by Bull under OEM. From now on, the terminology ‘target platform(s)’ or ‘target system(s)’ in this document will designate these platforms.

2.2 TOE Overview

The B1/EST-X product provides a complete multi-level environment, featuring:

- Mandatory access control
- Discretionary access control
- Identification and authentication (I&A)
- Audit
- Data interchange (import/export)

The B1/EST-X product contains additional features over and above the claims being made and evaluated in this document. These include TCP/IP based communications facilities.

B1/EST-X Security Status

The B1/EST-X product is based on the AIX operating system, with an additional security module loaded at system installation time.

B1/EST-X systems offer all ITSEC F-B1 functionality class features. The B1/EST-X product is currently limited to the F-B1 functionality class because the Trusted Computing Base (TCB) has not been re-structured for modularity and a covert channel analysis has not been performed.

Mandatory Access Control (MAC)

The B1/EST-X solution for mandatory access control allows most users to work on the system without being cognizant of the controls, yet allows the administrator to monitor and protect information at multiple MAC levels. The supports system up to 256 hierarchical classifications and up to 128 non-hierarchical compartments.

The B1/EST-X product labels every object (file, device) with a MAC label and enforces mandatory access control between all subjects (processes) and objects.

The B1/EST-X product enforces a hierarchical directory tree with increasing MAC levels of files descending in the hierarchy. Thus, every file and directory dominates the MAC level of its parent directory. The B1/EST-X product implements multilevel directories for those directories which are shared by convention in traditional UNIX, e.g., **/tmp.** Each directory is actually a collection of directories, each of which contains all files at a single MAC level. This technique is used to implement all directories which are conventionally shared in UNIX. A user can only see files whose MAC level is the same as the process MAC level. Administrative programs, such as spooling programs, can view files in all directories to collect work from all users on the system. Thus, regular users are given the impression that **/tmp** contains files at their MAC level only, while administrative users can manipulate the collection of directories which together implement **/tmp**.

The use of each device is under the control of the administrator. The ITSEC specifies different treatment for single- and multi-level devices, with different handling requirements for each. For tapes, the administrator controls the maximum MAC level of information imported to, or exported from, that device. Physical controls over access to printers define the maximum level of information to be printed, as well as whether single- or multi-level information can be printed. Each device node in the file system is assigned according to the requirements of the Security Officer.

The B1/EST-X product associates a current MAC level and clearance with each user process. A process may only write to a file that is at the same MAC level as the process. A user may not see the contents of a file that is above his clearance. User clearances are managed by the administrator and are stored together with all the additional per-user and system-wide parameters.

Discretionary Access Control (DAC)

The B1/EST-X product provides the traditional UNIX features that allows read, write and execute (search) permissions for the owner, the group, and others (OGO protection). Also provided is a system of discretionary access controls based on access control lists, giving finer granularity of control. These have been introduced in such a way that compatibility with traditional UNIX is maintained for those users who do not require to use them and for those applications that are ignorant of them.

Identification and Authentication (I&A)

The B1/EST-X product implements the password recommendations of the DoD NCSC Green Book. The security officer determines whether users can select their own passwords or must use a password generated by the system. In the latter case, an algorithm must be provided for the generation of random passwords meeting the security officer’s requirements.

Audit

The B1/EST-X product includes a highly configurable audit system. Auditing is divided into two general areas: audit collection and audit reduction. (In [ITSEC] these areas are

referred to as “accountability” and “audit” respectively.) The generation of audit records, or audit collection, is divided into many different audit events. Each audit event is controlled by system default and per-user audit masks. This granularity allows the administrator to generate only the audit information required at that site, minimizing the size of the audit trails.

The audit system has minimal overhead, as the audit data is buffered within the kernel and sent to an audit daemon outside the kernel. The audit daemon then compacts the data and writes it to a file. The size of the buffers, use of compaction, and other parameters are all configured by editing text files.

In addition to the pre-defined audit events, applications can generate their own audit records and add them to the system audit trail.

Data Interchange (Import/Export)

The import/export features of the B1/EST-X product allow the system to produce and manipulate magnetic export media. In addition, printed information is labeled so that it can be physically handled in accordance with its MAC label. The B1/EST-X product recognizes the following tape formats:

- Traditional *tar* and *cpio*
- POSIX-compliant *pax*
- Multilevel *lpax*

The Security Officer, designates each tape device as single- or multi-level (unlabeled or labeled) formats. Labeled formats include a tape header which describes the security configuration of the system and parameters for each configured security policy, and a body which describes the security parameters of each field preceding the file's contents.

A new utility, *lpax*(1) based on the POSIX portable archiver *pax*, has been implemented to manipulate multi-level media. This assures that the use of each device is consistent with its assignment. *lpax* recognizes ordinary tar, cpio, and pax formats, and creates multi-level archives based on the pax format.

The backup and restore utilities may also be used for import and export of labeled data, but these are only available to the root user and are only intended for use in system installation and in the manufacture of installable media. Since the root user is allowed to bypass MAC controls, MAC mediation has not been implemented in these utilities.

The import and export channels supported by the TOE are diskette and tape devices.

Object Reuse

The B1/EST-X product satisfies the ITSEC F/B1 requirements for object reuse. For each type of object, this is achieved in one of two ways: either each instance of the object type is cleaned before being reissued, or else the interface to it is designed in such a way that it is semantically impossible to read data that has not been written by the same user. The object reuse mechanism is totally transparent and is invoked automatically. It cannot be disabled, even by an administrator.

3 Security Environment

This section identifies the security issues which govern the choice of the security requirements in this ST. It identifies the threats to the data security which the TOE is

intended to counter, security policies for which the TOE is appropriate, and the secure usage assumptions in terms of physical, personnel and other aspects of the environment of the TOE.

3.1 Secure Usage Assumptions

The TOE is assured to provide effective security measures only if it is installed, managed, and used correctly. The operational environment must be managed according to the requirements set forth in the TOE's documentation for delivery, operation, and user and administrator guidance, according to the assurance requirements of level EAL4.

The following specific conditions are assumed to exist in the TOE's environment:

3.1.1 Physical Assumptions

The TOE is intended for application in user areas that have physical control and monitoring. It is assumed that the following physical conditions will exist:

A.LOCATE The processing resources of the TOE will be located within controlled access facilities which will prevent unauthorized physical access.

A.PROTECT The TOE hardware and software critical to security policy enforcement will be physically protected from unauthorized modification by potentially hostile outsiders.

3.1.2 Personnel Assumptions

It is assumed that the following personnel conditions will exist:

A.NO_EVIL Administrators are assumed to be non-hostile and trusted to perform their duties correctly.

A.ACCESS Users possess the necessary privileges to access the information managed by the TOE.

3.1.3 Intended Usage Assumptions

A.AUDIT Achievement of assurance level EAL4 and functionality class F-B1 depends on the auditing capabilities of the TOE being active and configured in a certain way. Specifically, auditing must be configured such that it is automatically enabled on system boot, and the system is shut down if disk space for the audit trail is exhausted. This ensures that it is impossible for auditing to cease without the administrator being aware of the fact. The TOE is set into this configuration during installation.

A.TERM In order to achieve the EAL4 level of assurance, the system must be used with Qume QVT61 terminals operating in VT220 mode only, or terminals which emulate QVT61 VT220 mode completely.

A.MAC The "MAC override" facility, whereby a given set of users may be specified as having the ability to override MAC mediation (normally only available to

the root user) is not evaluated and must not be used if the system is to conform to the evaluated configuration.

3.1.4 Connectivity assumptions

The ST contains no explicit network or distributed system requirements. However, it is assumed that the following connectivity conditions exist:

A.PEER Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints.

The ST is applicable to networked or distributed environments only if the entire network operates under the same constraints and resides within a single management domain. There are no security requirements which address the need to trust external systems or the communications links to such systems.

A.CONNECT All connections to peripheral devices reside within the controlled access facilities.

The ST only addresses security concerns related to the manipulation of the TOE through its legitimate interfaces. Internal communication paths to interface points such as terminals are assumed to be adequately protected.

3.2 Threats to Security

The TOE is able to counter threats which may be broadly categorized as the threat of attack from hostile outsiders with no legitimate access to the system, and threats from insiders with legitimate access to the system attempting to gain access to and perform operations on objects for which they have no individually defined rights. In addition, certain threats of a non-IT nature can affect the security of the TOE and must be dealt with by the operating environment.

3.2.1 Threats addressed by TOE

The B1/EST-X product is extremely rich in security functionality. It is the intention of the following sections to state the threats that the system could be under, and which it would be expected to withstand.

Identification & Authentication

T.IA-1: Person gaining access to the system without being correctly identified or authenticated.

T.IA-2: User gaining access to the authentication data for subversive purposes (e.g. reading password file for cryptographic attack).

T.IA-3: A user assuming the identity of another user once access has been granted to the TOE.

T.IA-4: An attacker attempts to guess a valid user/password combination by a random or systematic search through all possibilities.

Access Control

T.AC-1: The MAC level for a subject or an object is unspecified or not determined with the result that mandatory access controls cannot be enforced.

T.AC-2: A subject acquires a MAC label which dominates his clearance.

T.AC-3: Data is downgraded by being read by a subject which does not have sufficient clearance, or written to a file having lower MAC level than the subject.

T.AC-4: Data being printed without a suitable marking to reflect the MAC label of the object from which it originated.

T.AC-5: User gaining access to data which the owner has not granted the user the required access.

T.AC-6: User attempts to change the owner or group of an object, not being the owner himself and not having been granted permission to do so by the owner.

T.AC-7: User attempts to change the access permissions (OGO or ACL) of an object, not being the owner himself and not having been granted permission to do so by the owner.

T.AC-8: An object exported and later imported to the TOE or to another multi-level system loses its MAC label in transit.

T.AC-9: Inadvertent downgrade of data when content of an object is transferred unlabelled via a single-level.

T.AC-10: Unlabelled data re-imported to the TOE or imported from another system is given inappropriate MAC label.

Audit & Accounting

T.AA-1: User performing any security relevant action without being detected.

T.AA-2: Unauthorized user modifying or deleting the audit trail.

Object Reuse

T.OR-1: User attempts to read dynamically allocated memory, area of file not yet written, or IPC channel in order to obtain information regarding other user processes.

3.2.2 Threats to be addressed by the operating environment

The threat possibilities discussed below must be countered in order to support the TOE security capabilities but are not addressed directly by the TOE itself. Such threats must be addressed by the operating environment.

T.INSTALL The TOE may be delivered and installed in a manner which undermines security.

The security offered by TOE is predicated upon the TOE being initially established in a secure state. That includes assurance that the TOE delivered is that which was evaluated and that the TOE is subsequently installed properly.

T.OPERATE Security failures may occur because of improper administration and operation of the TOE.

The security offered by the TOE can be assured only to the extent that the TOE is operated correctly by system administrators and authorized users.

Users or external threat agents may, through accidental discovery or directed search, discover inadequacies in the security administration of the TOE which permit them to gain logical access to its resources in breach of any permissions they may have.

Potential attackers may seek to develop methods whereby the improperly administered security functions of the TOE may be circumvented during normal operation.

T.PHYSICAL Security-critical parts of the TOE may be subjected to physical attack which may compromise security.

The security offered by the TOE can be assured only against attacks on the TOE which seek to exploit its legitimate interfaces. It is therefore assumed that adequate physical controls are in place to prevent potential attack agents from gaining access to the TOE or the platform upon which the TOE is operating.

3.3 Organizational Security Policies

Within government environments, the TOE is suitable to protect multi-level classified information as it is designed to enforce controls on the flow of information between objects at differing levels of information sensitivity.

For commercial environments, the TOE is suitable to protect information in situations in which availability of that information needs to be restricted such that only designated users may access the information.

Because the security objectives are directly derived from the threats stated above there is no explicit statement of organizational security policies.

4 Security Objectives

4.1 Security Objectives for the TOE

The following are the TOE IT security objectives:

O.I&A The TOE must uniquely identify all users, and must authenticate the claimed identify before granting a user access to the TOE facilities.

O.DAC The TOE must provide its users with the means of controlling access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users, and in accordance with the set of DAC rules.

O.MAC The TOE must protect the confidentiality of information it is responsible for managing, in accordance with the MAC rules, based directly on comparison of an individual's clearance or authorization for the information, and the sensitivity designation of the information.

O.LABEL The TOE must store and preserve the integrity of sensitivity labels for information it stores and processes. Data output (exported) by the TOE must have sensitivity labels that are an accurate representation of the corresponding internal sensitivity labels.

O.AUDIT The TOE must provide the means of recording any security relevant events, so that an administrator can detect potential attacks or misconfiguration of the TOE security features that would leave the TOE susceptible to attack, and also hold users accountable for any actions they perform that are relevant to security.

4.2 Security Objectives for the Environment

The TOE is assumed to be complete and self-contained and, as such, is not dependent upon any other products to perform properly. However, certain objectives with respect to the general operating environment must be met in order to support the TOE's security capabilities.

The following are the non-IT security objectives:

O.INSTALL Those responsible for the TOE must ensure that the TOE is delivered and installed in a manner which maintains IT security.

O.MANAGE Those responsible for the TOE must ensure that it is managed, administered and operated in a manner which maintains IT security.

O.PHYSICAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack which might compromise IT security.

O.CREDEN Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which maintains IT security.

O.CONN Those responsible for the TOE must ensure that no connections to outside systems or users can undermine the IT security objectives.

5 IT Security Requirements

This section contains functional and assurance requirements that are satisfied by the TOE. These requirements consist of functional components from Part 2 of the Common Criteria and an Evaluation Assurance Level (EAL) containing assurance components from Part 3.

5.1 TOE Security Functional Requirements

The B1/EST-X product implements all the security enforcing functions of ITSEC F-B1, as specified in [ITSEC].

5.1.1 Identification and Authentication

FIA_UID.2 **Basic User Identification**

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 **Basic User Authentication**

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.

FMT_MTD.1 (1) **Management of TSF Data**

FMT_MTD.1.1 The TSF shall restrict the ability to *observe, modify and destruct* the *following* security attributes:

the user authentication data related to the password mechanism at all times while it resides in the TOE

to

the authorized administrator and to all authorized users, where each user is restricted to observe, modify and destruct only his own authentication data in accordance with the TSP

Refinement:

The password mechanism shall store passwords in a one-way encrypted form.

The user identity and login user identity must be unique.

Users will be provided with information on the last successful and unsuccessful attempts to use their accounts.

Password lifetimes may be specified, forcing users to change their passwords after a set period before any subjects can be activated on their behalf.

The TOE supports the automatic locking of terminals or user accounts after a set number (configurable only by an administrator) of consecutive rejected login attempts.

FMT_SMR.1 **Security roles**

FMT_SMR.1.1 The TSF shall maintain the roles[1]

privileged administrator

unprivileged user

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

FIA_USB.1 **User-Subject Binding**

FIA_USB.1.1 The TSF shall associate the appropriate *user identity attributes* with subjects acting on behalf of that user.

FIA_ATD.1 **User Attribute Definition**

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

user identity attributes

FMT_MTD.1 (2) **Management of TSF Data**

FMT_MTD.1.1 The TSF shall restrict the ability to *add, delete or suspend* the:

user identities known to the TOE

to

the authorised administrator.

5.1.2 Discretionary Access Control

FDP_ACC.1 **Subset Access Control**

FDP_ACC.1.1 The TSF shall enforce the *Discretionary Access Control (DAC) SFP* on:

system subjects

a) users

b) processes acting upon behalf of users

controlled objects

a) controlled file system objects

b) controlled IPC objects

[1] although AIX/B1/EST-X provide administrative roles they are not stated here, because they are not required by F-B1.

Refinement:

operations among system subjects and controlled objects covered by the DAC SFP:

a) read

b) write

c) execute or directory search

FMT_MSA.1 (1) **Management of Security Attributes**

FMT_MSA.1.1 The TSF shall enforce the *Discretionary Access Control Policy* to restrict the ability to *modify* the security attributes:

object security attributes

to

a) the authorised administrator

b) the owner of the object (B1/EST-X specific: chown only for super-user)

FDP_ACF.1 **Security Attribute Based Access Control**

FDP_ACF.1.1 The TSF shall enforce the *Discretionary Access Control Policy* on objects based on *the following DAC attributes*:

process DAC attributes:

a) effective user identity

b) effective group identity and supplementary group identities

object security attributes:

a) object owner class

b) object group class

c) object permission bits (Base ACL)

d) extended ACL

e) IPC objects only: object creator class, object creator group class

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

1. If the UID is equal to that of the system administrator then

a) in case a read, write or traverse access right is requested, access is granted.

b) in case a execute access right is requested, access is granted only if for at least one of the classes (owner, group, others) or by some access control entry the execute right is enabled, otherwise access is denied.

c) access mediation ends here.

2. If the UID and/or GIDs of the requesting user match the current access control entry (in the extended ACL part information by either being the user u and belonging to all of the groups g1, g2 ...., respectively by belonging to all of the groups g1, g2 .... if no user is specified) then

a) in case the requested access right is explicitly denied or specified as "-", access is denied, even when it was marked as "permitted" before. Access mediation ends here.

b) in case the requested access right is permitted, it is marked as "permitted".

c) otherwise (no match), get the next access control entry and goto 2.

3. At this point the requested access is either marked as permitted or there was no matching entry in the extended ACLs. Next the base ACL is checked.

4. If the UID is equal to that of the owner of the object then

a) in case the requested access right is enabled for the class "owner", access is granted otherwise denied (even when the access right was marked as "permitted").

b) access mediation ends here.

5. If one of the GIDs is equal to that associated with the object then

a) in case the requested access right is enabled for the class "group" or has been marked as "permitted" before, access is granted otherwise denied.

b) access mediation ends here.

6. If the UID and the GIDs of the process do not meet any of the conditions 4 and 5, the process represents a user of class "others". In case the requested access right is enabled for the class "others" or has been marked as "permitted" before, access is granted otherwise denied.

When access is granted the process and therefore the associated user get an object descriptor. The system ensures via the object descriptor that further access requests on that object do not go beyond the granted access modes.

If a process executes a program having the setuid or setgid bit set, the process will assume the effective user or effective group id of the program for the duration of the execution.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *no additional rule:*

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *no additional rules*

FMT_MSA.3 (1) Static Attribute Initialisation

FMT_MSA.3.1 The TSF shall enforce the *Discretionary Access Control Policy* to provide *inherited (owner/group) and user definable (ACLs)* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the *authorised user* to specify alternative initial values to override the default values when an object or information is created.

5.1.3 Mandatory Access Control

FDP_IFC.1 **Subset Information Flow Control**

FDP_IFC.1.1 The TSF shall enforce the *Mandatory Access Control (MAC) SFP* on:

system subjects

a) users

b) processes acting upon behalf of users

controlled objects

a) controlled file system objects

Refinement:

operations among system subjects and controlled objects covered by the MAC SFP:

a) read

b) write

FDP_IFF.2 **Hierarchical Security Attributes**

FDP_IFF.2.1 The TSF shall enforce the *Mandatory Access Control (MAC) SFP* to enforce at least the following types of subject and information security attributes:

subject security attributes:

MAC label, consisting of

a) classification

b) category

information security attributes:

MAC label, consisting of

a) classification

b) category

FDP_IFF.2.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules based on the ordering relationships between security attributes hold:

The attribute consists of two parts. Part one (classification) has hierarchically ordered values, part two (category) represents a set.

An attribute A is said to dominate an attribute B if:

Part one of A is hierarchically greater than, or equal to, part one of B and part two of B is a proper subset of, or equal to, part two of A.

The following rules are enforced:

a) Read access by a subject to an object is only permitted if the attribute of the subject dominates that of the object.

b) Write access by a subject to an object is only permitted if the attribute of the object equals that of the subject.

FDP_IFF.2.3 The TSF shall enforce *the DAC SFP additional to the MAC SFP:*

FDP_IFF.2.4 The TSF shall provide the following capabilities:

Text files (that may only be set up or modified by an administrator) define all of the classifications and categories used to construct MAC labels on the system. These files also define the external representations of the classifications and categories, with exception of the predefined MAC labels SYSTEM_LOW, SYSTEM_HIGH and WILDCARD. (More than one external representation may be defined for a classification, but not for a category.).

Only a privileged subject can regrade an object.

To designate a directory as multilevel/single level:
- the process must have superuser privilege
- the directory must be empty.

The only objects that can be regraded (subject to TF[12.2]) are directories, device files.

FDP_IFF.2.5 The TSF shall explicitly authorise an information flow based on the following additional rules: *no additional rule:*

FDP_IFF.2.6 The TSF shall explicitly deny an information flow based on the following additional rules: *no additional rules*

FMT_MSA.3 (2) Static Attribute Initialisation

FMT_MSA.3.1 The TSF shall enforce the *Mandatory Access Control Policy* to provide *inherited* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow *nobody* to specify alternative initial values to override the default values when an object or information is created.

5.1.4 Data Import/Export

FDP_ETC.1 **Export of user data without security attributes**

FDP_ETC.1.1 The TSF shall enforce the *Mandatory Access Control (MAC) SFP* when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

FDP_ETC.2 **Export of user data with security attributes**[2]

FDP_ETC.2.1 The TSF shall enforce the *Mandatory Access Control (MAC) SFP* when exporting user data, controlled under the SFP, outside of the TSC.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TSC:

Each export channel shall be identifiable as either single-level or multi-level. (The only import/export channels supported are diskette and tape drives.) It shall be impossible to transmit or receive data via channels designated as single-level, unless the attributes of that data match a fixed pre-specified attribute (the pre-specified attribute being derived from the attribute of the device).

For a single-level channel it is possible for an authorised user to specify the attribute of the channel in a way that cannot be imitated. The attribute of the data is implicitly specified by the attribute of the channel (and the data is exported unlabelled).

For multi-level channels it shall be ensured by the communication protocol that the recipient can completely and unambiguously reconstruct and pair the received data and attributes. (By "communication protocol" is meant the data and label encoding used by the import/export utility).

Unauthorized users shall not be able to change the security relevant attributes of a channel. It shall not be possible to change these attributes without the change being performed explicitly.

---

[2] this requirement applies only to the l*pax* utility

The TOE shall mark human readable output with attribute values. The values of the attributes shall be determined according to the rules laid down in the TOE.

Authorized users shall be able to specify the printable name of each attribute value.

FDP_ITC.1 **Import of user data without security attributes**

FDP_ITC.1.1 The TSF shall enforce the [assignment: access control SFP and/or information flow control SFP] when importing user data, controlled under the SFP, from outside of the TSC.

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

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC:

Upon unlabelled import, MAC labels are inherited from the process performing the import

FDP_ITC.2 **Import of user data with security attributes**[3]

FDP_ITC.2.1 The TSF shall enforce the *Mandatory Access Control (MAC) SFP* when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC:

For multi-level channels it shall be ensured by the communication protocol that the recipient can completely and unambiguously reconstruct and pair the received data and attributes. (By "communication protocol" is meant the data and label encoding used by the import/export utility).

Unauthorized users shall not be able to change the security relevant attributes of a channel. It shall not be possible to change these attributes without the change being performed explicitly.

[3] this requirement applies only to the l*pax* utility

A user's group determines whether he is authorized to perform import/export operations, and the MAC labels on a device determine what files can be imported or exported through it.

On multi-level channels: The files that can be imported lpax is limited by the relationship of the device MAC label range and the user's clearance to the MAC labels of the files.

FMT_MSA.1 (2) Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the *Mandatory Access Control Policy* to restrict the ability to *modify* the security attributes:

channel security attributes

to

a) the authorized administrator

5.1.5 Accountability and Audit

FAU_GEN.1 Audit Data Generation

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) All auditable events for the *minimum* level of audit:

FIA_UID.2: Unsuccessful use of the identification mechanism, including the user identity provided. (USER_Login)

FIA_UAU.2: Unsuccessful use of the authentication mechanism. (USER_Login)

FIA_USB.1: Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject). (PROC_Create, PROC_RealUID, PROC_AuditUID, PROC_SetUserIDs, MAC_Setproc, MAC_Setclrance, MAC_SetB1Priv)

FDP_ACF.1: Successful requests to perform an operation on an object covered by the SFP. (all FILE_* events)

FDP_IFF.2: Decisions to permit requested information flows. (all FILE_* events)

FDP_ETC.2: Successful export of user data, including any security attributes. (LPAX_Archive)

FDP_ITC.2: Successful import of user data, including any security attributes. (LPAX_Archive)

FAU_SEL.1: All modifications to the audit configuration that occur while the audit collection functions are operating. (AUD_CONFIG_WR)

FMT_SMR.1: modifications to the group of users that are part of a role. (S_PASSWD_WRITE, S_USER_WRITE)

FPT_STM.1: changes to the time. (PROC_Settimer, PROC_Adjtime)

Refinement:

It is possible to configure the TOE so that auditing is automatically started at system boot time, and so that the TOE shuts down automatically if space for the audit trail is exhausted. (The TOE shall be so configured.)

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 PP/ST,

MAC label of object if applicable

MAC label of subject if applicable

FIA_UID.2: user name and terminal

FIA_UAU.2: user name and terminal

FIA_USB.1: process id, involved user ids, level, privilege

FDP_ACF.1: object name/descriptor

FDP_IFF.2: object name/descriptor

FDP_ETC.2: command name

FDP_ITC.2: command name

FAU_SEL.1: file name

FMT_SMR.1: file name

FPT_STM.1: old and new time.

FPT_STM.1 Reliable time stamps

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

FAU_GEN.2 User Identity Generation

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_SEL.1 Selective Audit

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) user identity (B1/EST-X is able for more, but this is beyond F-B1)

FMT_MTD.1 (3) **Management of TSF data**

FMT_MTD.1.1 The TSF shall restrict the ability to

query, modify, clear

the

audit trail

and to

modify

the

audit configuration

to

the privileged administrator

FAU_SAR.1 **Audit Review**

FAU_SAR.1.1 The TSF shall provide *authorised users* with the capability to read *any audit information* from the audit records.

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

FAU_SAR.3 **Selectable Audit Review**

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

a) user identity

5.1.6 Object Reuse

FDP_RIP.2 **Full Residual Information Protection**

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.

5.1.7 Additional Functions Required by CC

Some functional requirements as stated above are the result of dependency requirements of the CC and are not explicitly required by F-B1, e.g. reliable time stamps.

5.2 IT Assurance requirements

The assurance requirements for the TOE are portrayed in Table 2 below. The assurance augmentation components are described following the table:

Requirement	Name
EAL4	Methodically Designed, Tested, and Reviewed
ALC_FLR.2	Flaw Reporting Procedures

Table 2: Assurance Requirements

ALC_FLR.2 Flaw reporting procedures

Developer action elements:

ALC_FLR.2.1D The developer shall document the flaw remediation procedures.

ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon user reports of security flaws and requests for corrections to those flaws.

Content and presentation of evidence elements:

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information and corrections to TOE users.

ALC_FLR.2.5C The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.

ALC_FLR.2.6C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

Evaluator action elements:

ALC_FLR.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3 Security Requirements for the IT Environment

There are no additional security requirements on the IT environment the TOE depends on.

6 TOE Summary Specification

6.1 Statement of TOE IT Security Functions

The TOE IT security functions in this section are stated as trusted functions (TFs) implemented by the TOE, which are taken from the B1/EST-X supplementary documentation. These are mapped to security enforcing functions as known from the functionality class ITSEC F-B1 and also to the security function requirements (SFRs) taken from the CC.

6.1.1 Identification and Authentication

The following table maps the trusted TOE functions (TFs) to CC security function requirements (SFRs). The numbering of the TFs implicitly map them to SEFs taken from ITSEC F-B1. TF number [x.y] means TF number y related to SEF x. The SEFs related to Identification and Authentication are as follows:

SEF1 The TOE shall uniquely identify and authenticate users.

SEF2 Identification and authentication shall take place prior to all other interactions between the TOE and the user. Other interactions shall only be possible after successful identification and authentication.

SEF3 The authentication information shall be stored in such a way that it can only be accessed by authorized users.

SEF4 For every interaction, the TOE shall be able to establish the identity of the user.

SEF10 The actions for adding and deleting user identities known to the TOE, and the action to temporarily suspend all of a user's access rights, shall be restricted to authorised users.

Trusted TOE Function	**CC SFR**
TF: Users will be identified by a user identity and password combination [1.1].	FIA_UID.2, FIA_UAU.2
TF: The user identity and login user identity must be unique [1.2].	FMT_MTD.1 (1)
TF: Login attempts that are not authenticated are rejected [1.3].	FIA_UAU.2
TF: An unsuccessful login attempt must not provide any information useful to an attacker about the reason for rejection [1.4].	FIA_UID.2, FIA_UAU.2
TF: Users will be provided with information on the last successful and unsuccessful attempts to use their accounts [1.5].	FMT_MTD.1 (1)
TF: Rejected login attempts will be audited [1.6].	FAU_GEN.1
TF: Passwords may be system-generated or user-supplied (the	FMT_MTD.1 (1),

Trusted TOE Function	CC SFR
latter being the default). This is configurable only by the administrator, on a system-wide basis. (The password generation algorithm, including its user interface, is not itself part of the TOE.) Only an administrator can select a password for a new or forgetful user. [1.7].	FMT_SMR.1
TF: Password lifetimes may be specified, forcing users to change their passwords after a set period before any subjects can be activated on their behalf. [1.8].	FMT_MTD.1 (1)
TF: The TOE supports the automatic locking of terminals or user accounts after a set number (configurable only by an administrator) of consecutive rejected login attempts. [1.9]	FMT_MTD.1 (1)
TF: Authentication of a valid user identity and password combination is necessary before access to the TOE is granted [2.1].	FIA_UAU.2
TF: The TOE supports the locking of user accounts and terminals at the discretion of the administrator [2.2].	FMT_MTD.1 (2)
TF: When the TOE detects logout, it shall ensure that no further interaction with the user takes place, and that the cycle of secure authentication will restart [2.3].	FIA_UID.2, FIA_UAU.2
TF: Authentication information, in the form of the security databases which store the security parameters used by the TOE, is protected against unauthorized access [3.1].	FMT_MTD.1 (1), FMT_SMR.1
TF: Cleartext of passwords are not visible at any time except when a selection of system generated passwords is being offered to the user to choose from. [3.2].	FMT_MTD.1 (1)
TF: It is possible for the administrator (only) to install a customer supplied encryption algorithm to supplement the protection of stored passwords. (No such algorithm is claimed by the TOE) [3.3].	FMT_SMR.1
TF: All user actions are identifiable to the level of a unique user, via the concept of the login user id, luid. [4.1].	FIA_USB.1, FIA_ATD.1
TF: The luid can only be initialized or altered by the superuser. [4.2].	FMT_SMR.1, FMT_MTD.1 (2)
TF: Utilities only available to an administrator are responsible for the allocation and de-allocation of user identities [10.1].	FMT_SMR.1, FMT_MTD.1 (2)
TF: Utilities only available to an administrator are responsible for suspending a user's right to access the TOE [10.2].	FMT_SMR.1, FMT_MTD.1 (2)

Table 3: I&A: Mapping between IT Security Functions and SFRs

6.1.2 Discretionary Access Control

The following table maps the trusted TOE functions (TFs) to CC security function requirements (SFRs). The numbering of the TFs implicitly map them to SEFs taken from ITSEC F-B1. TF number [x.y] means TF number y related to SEF x. The SEFs related to Discretionary Access Control are as follows:

SEF 5: The TOE shall be able to distinguish and administer access rights between each user and the objects which are subject to the administration of rights, on the basis of an individual user, or on the basis of membership of a group of users, or both.

SEF 6: It shall be possible to completely deny users or user groups access to an object. It shall also be possible to restrict a user's access to an object to those operations which do not modify it.

SEF 7: It shall be possible to grant the access rights to an object down to the granularity of an individual user.

SEF 8: It shall not be possible for anyone who is not an authorised user to grant or revoke access rights to an object.

SEF 9: The administration of rights shall provide controls to limit propagation of access rights.

SEF 23: With each attempt by users or user groups to access objects which are subject to the administration of rights, the TOE shall verify the validity of the request. Unauthorised access attempts shall be rejected.

Trusted TOE Function	**CC SFR**
TF: Every object is labelled with one owner and one group. A subject may assume any group identity within its assigned set. [5.1]. *Applies also to SEF6.*	FDP_ACC.1, FDP_ACF.1
TF: An object inherits its owner/group combination from the effective identity of the process that creates it, except in the case of a file system object created in a directory which has the group inheritance flag set. Such an object inherits the owning group of the directory. [5.2].	FMT_MSA.3
TF: Only the superuser may transfer object ownership of a file system object from one user to another. Only the superuser, the creator or the owner may transfer object ownership of an IPC object from one user to another. [5.3].	FMT_MSA.1 (1)
TF: Any operation mediated by Discretionary Access Control that is permitted for an object's owner is also permitted, upon that object, for the superuser. [5.4].	FDP_ACF.1
TF: Discretionary Access Control permissions applying to an object grant or deny a subject the right to perform actions (as appropriate to the type of object) upon that object. [5.5]. *Applies also to SEF6.*	FDP_ACC.1, FDP_ACF.1
TF: Inter-process communications (IPCs) have a creating user and group as well as an owner; both of whom are regarded as "owners" for	FDP_ACC.1, FDP_ACF.1

Trusted TOE Function	CC SFR
the purposes of Discretionary Access Control. On creation the owner and creator identities are the same. The creator identity cannot be changed, even by the superuser.[5.6]	
TF: If a process executes a program having the setuid or setgid bit set, the process will assume the effective user or effective group id of the program for the duration of the execution. [5.7]	FDP_ACF.1
TF: An ACL may be applied to a file system object, specifying read, write and execute permissions for each of an arbitrary set of users/groups. [7.1].	FDP_ACC.1, FDP_ACF.1
TF: If an ACL is applied to a file system object, both the OGO and ACL are consulted, with restrictive modes taking precedence over permissive ones. The policy is fully described in User Documentation (Secure Features Users Guide). [7.2]	FDP_ACF.1
TF: It is not possible for anyone who is not an authorised user to grant or revoke access rights to an object [8.1].	FMT_MSA.1 (1)
TF: Only the owner of an object (or the superuser) can change the access right to an object, so conferring those rights on another subject. [9.1]	FMT_MSA.1 (1)
TF: Whenever a subject attempts to access an object the TOE performs an access check, considering all applicable OGO and ACL permissions, before access to the object is granted. [23.1]	FDP_ACF.1

Table 4: DAC: Mapping between IT Security Functions and SFRs

6.1.3 Mandatory Access Control

The following table maps the trusted TOE functions (TFs) to CC security function requirements (SFRs). The numbering of the TFs implicitly map them to SEFs taken from ITSEC F-B1. TF number [x.y] means TF number y related to SEF x. The SEFs related to Discretionary Access Control are as follows:

SEF 11: The TOE shall provide all subjects and storage objects (e.g. processes, files, storage segments, devices) under its control with attributes. The values of these attributes shall serve as a basis for mandatory access rights.

SEF 12: Rules shall specify which combinations of attribute values of subject and object are necessary for a subject to be granted access to that object.

SEF 14: The mandatory access rights shall be designed in such a manner that the following special case can be realized:

> The attribute consists of two parts. Part one has hierarchically ordered values, part two represents a set. (In the official world part one contains classifications e.g. unclassified, confidential, secret, top secret. Part two contains categories.)
>
> An attribute A is said to dominate an attribute B if:

Part one of A is hierarchically greater than, or equal to, part one of B and part two of B is a proper subset of, or equal to, part two of A.

The following rules are enforced:

a) Read access by a subject to an object is only permitted if the attribute of the subject dominates that of the object.

b) Write access by a subject to an object is only permitted if the attribute of the object dominates equals that of the subject.

SEF 15: The attributes of a subject created to act on behalf of a user shall be dominated by that user's clearance and authorization as determined at identification and authentication time. (“Authorization” is taken to mean the same as “clearance”.)

SEF 24: The values of the attributes shall serve as a basis for decisions concerning mandatory access control. The rules shall unambiguously specify when a subject is allowed access to such a protected object. *Essentially the same as SEF12, therefore covered by TF12.x*

SEF 25: If discretionary access rights are also assigned for an object, access shall only be permitted provided that both the discretionary and mandatory access rights allow such access.

Trusted TOE Function	**CC SFR**
TF: All subjects (process) have a MAC label, (established when they are created) denoting the current MAC level at which the process is executing. There also exists a clearance label associated with every account, denoting the clearance level of the user on whose behalf the subject is running. [11.1]	FDP_IFC.1
TF: Whenever the TOE creates an object, it associates a MAC label with it. [11.2]	FDP_IFC.1
TF: Subjects and Objects inherit their MAC labels from the processes that create them. [11.3]	FMT_MSA.3 (2)
TF: Files (i.e. all file system objects except directories) can be labelled with a WILDCARD MAC label, which allows any process MAC access to the object. [11.4]	FMT_MSA.3 (2)
TF: The File System Invariant: The MAC label of a file system object dominates the MAC label of the directory (single or multilevel) in which it is contained. Except for directories and devices, file system objects have the same MAC label as their parent directories. (Even the superuser is bound by this invariant.) [11.5]	FDP_IFF.2
TF: Text files (that may only be set up or modified by an administrator) define all of the classifications and categories used to construct MAC labels on the system. These files also define the external representations of the classifications and categories, with exception of the predefined MAC labels SYSTEM_LOW, SYSTEM_HIGH and WILDCARD. (More than one external representation may be defined for a classification, but not for a	FDP_IFF.2

category.) [11.6]	
TF: The TOE compares the MAC labels of the subject and object when making any access decision. [12.1]	FDP_IFF.2
TF: Only a privileged subject can regrade an object. [12.2]	FDP_IFF.2
TF: Only a process that has the same MAC label as a directory can create an object in it, unless the object is a directory or a device file and the process dominates the label of the directory. [12.3]	FDP_IFF.2
TF: To designate a directory as multilevel/single level: - the process must have superuser privilege - the directory must be empty. [12.4]	FDP_IFF.2
TF: A process with privilege cannot create a file of any type in a multilevel parent directory. The only files that can be created are the multilevel child directories that the TOE automatically creates when a process that does not have privilege searches, reads or writes to the multilevel parent directory. [12.5]	FDP_IFF.2
TF: The only objects that can be regraded (subject to TF[12.2]) are directories, device files. [12.6]	FDP_IFF.2
TF: The TOE establishes one of the following relationships between a pair of MAC labels A and B: - A strictly dominates B (i.e. A's classification is greater then B's and B's category set is a proper subset of A's category set). - B strictly dominates A. - A and B are equal. - A and B are incomparable. [14.1]	FDP_IFC.1, FDP_IFF.2
TF: Users' security attributes are mediated by values taken from the authentication profile database at the time of the start of a login session. [15.1]	FDP_IFF.2
TF: If discretionary access rights are also assigned for an object, access is only permitted provided that both the discretionary and mandatory access rights allow such access, as demanded by TF[23.1] and TF[12.1]. [25.1]	FDP_ACF.1, FDP_IFF.2

Table 5: MAC: Mapping between IT Security Functions and SFRs

6.1.4 Data Import/Export

The following table maps the trusted TOE functions (TFs) to CC security function requirements (SFRs). The numbering of the TFs implicitly map them to SEFs taken from ITSEC F-B1. TF number [x.y] means TF number y related to SEF x. The SEFs related to Data Import/Export are as follows:

SEF 13: When exporting an object its attributes shall be exported in such a way that the recipient can reconstruct their value unambiguously.

SEF 16: If imported data does not have attributes, an authorized user shall be able to assign attributes to the data.

SEF 17: Each export channel shall be identifiable as either single-level or multi-level. (The only import/export channels supported are diskette and tape drives.) It shall be impossible to transmit or receive data via channels designated as single-level, unless the attributes of that data match a fixed pre-specified attribute (the pre-specified attribute being derived from the attribute of the device).

SEF 18: For a single-level channel it is possible for an authorized user to specify the attribute of the channel in a way that cannot be imitated. The attribute of the data is implicitly specified by the attribute of the channel (and the data is exported unlabelled). *SEF covered by TF 17.3.*

SEF 19: For multi-level channels it shall be ensured by the communication protocol that the recipient can completely and unambiguously reconstruct and pair the received data and attributes. (By "communication protocol" is meant the data and label encoding used by the import/export utility).

SEF 20: Unauthorized users shall not be able to change the security relevant attributes of a channel. It shall not be possible to change these attributes without the change being performed explicitly.

SEF 21: The TOE shall mark human readable output with attribute values. The values of the attributes shall be determined according to the rules laid down in the TOE.

SEF 22: Authorized users shall be able to specify the printable name of each attribute value. *SEF covered by TF11.6.*

Trusted TOE Function	**CC SFR**
TF: An archiving utility is available which uses an "extended format archive" to create and restore archives containing MAC labels (as well as DAC permissions). [13.1]	FDP_ITC.2, FDP_ETC.2
TF: Upon unlabelled import, MAC labels are inherited from the process performing the import. [16.1]	FDP_ITC.1
TF: Two basic modes exist for the importing and exporting of data: - commands utilizing traditional archiving modes are supported (including tar, cpio and pax). These provide single level import/export. - non-traditional extended archive format that allows complete specification of all file attributes (provided by the lpax program) [17.1]	FDP_ITC.1, FDP_ITC.2, FDP_ETC.1, FDP_ETC.2
TF: A user's group determines whether he is authorized to perform import/export operations, and the MAC labels on a device determine what files can be imported or exported through it [17.2].	FDP_ITC.2, FDP_ETC.2
TF: The administrator (only) can modify or display the following information on each device: - The device designation (single-level or multilevel) for MAC labels; - The currently assigned MAC label if the device is designated single-level; - The minimum and maximum MAC labels if the device is	FMT_MSA.1 (2)

Trusted TOE Function	CC SFR
designated multilevel. [17.3]	
TF: Single level: A file is exported only if the user can access the file for reading. [17.4]	FDP_IFF.2
TF: Multilevel: The files that can be imported or exported by lpax is limited by the relationship of the device MAC label range and the user's clearance to the MAC labels of the files. [17.5]	FDP_IFF.2
TF: The security attributes stored in the extended format archive include the MAC label (held as a representation of the human-readable form). [19.1]	FDP_ITC.2, FDP_ETC.2
TF: A device to be used for labeled import/export must be configured as multilevel. (A single-level device cannot be used for labeled import/export.) [19.2]	FDP_ITC.2, FDP_ETC.2
TF: Software that manipulates extended format media can read extended format archives created on systems configured with a subset of the attributes defined on the importing TOE. [19.3]	FDP_ITC.2, FDP_ETC.2
TF: Unauthorized users are not able to change the security relevant attributes of a device. It is not possible to change these attributes without the change being performed explicitly (for example, the data passing though a device does not change its attributes). [20.1].	FMT_MSA.1 (2)
TF: The TOE ensures that internal page labels on printed output contain a textual representation of the MAC level of the printed data [21.1].	FDP_ETC.2
TF: The TOE ensures that whenever a banner page is printed, it contains the following items: the MAC label of the data contained in the printout the user name, printer name, date/time and job title [21.2].	FDP_ETC.2

Table 6: Data Import / Export: Mapping between IT Security Functions and SFRs

6.1.5 Accountability and Audit

The following table maps the trusted TOE functions (TFs) to CC security function requirements (SFRs). The numbering of the TFs implicitly map them to SEFs taken from ITSEC F-B1. TF number [x.y] means TF number y related to SEF x. The SEFs related to Accountability and Audit are as follows:

SEF26 The TOE shall contain an accountability component which is able, for each of the following events, to log that event together with the required data:

a) Use of the identification and authentication mechanism:

   Required data: date; time; user identity supplied; identification of equipment on which the identification and authentication mechanism was used (e.g., terminal-id); success or failure of the attempt; authorisation of the user.

b) Actions that attempt to exercise access rights to an object which is subject to the administration of rights:

   Required data: date; time; user identity; name of the object; type of access attempt; success or failure of the attempt; attribute of the object.

c) Creation or deletion of an object which is subject to the administration of rights:

   Required data: date; time; user identity; name of the object; type of action; attribute of the object.

d) Actions by authorised users affecting the security of the TOE:

   Required data: date; time; user identity; type of action; name and attribute of the object to which the action relates (such actions are introduction or deletion (suspension) of users; introduction or removal of storage media; start up or shut down of the TOE; assignation of an attribute; change of attributes, markings or classification of a channel).

SEF27 Unauthorised users shall not be permitted to access accountability data.

SEF28 It shall be possible to selectively account for the actions of one or more users.

SEF29 Tools to examine and to maintain the accountability files shall exist and be documented. These tools shall allow actions of one or more users to be identified selectively.

SEF30 Tools to examine the accountability files for the purpose of audit shall exist and be documented. These tools shall allow actions of one or more users to be identified selectively.

Trusted TOE Function	**CC SFR**
TF: Details of all auditable events will be recorded by the TOE in an audit trail. (Administration documentation contains a list of claimed auditable events.) [26.1].	FAU_GEN.1, FPT_STM.1
TF: Details recorded will include the MAC label(s) of the subject and/or object whenever these are referenced by the event [26.2].	FAU_GEN.1
TF: The luid is recorded for every security-relevant action, and ensures that the action can be traced back to its originator [26.3].	FAU_GEN.1, FAU_GEN.2
TF: An administrator (only) will be able to specify which event types are to be audited [26.4].	FMT_MTD.1 (3)
TF: It is possible to configure the TOE so that auditing is automatically started at system boot time, and so that the TOE shuts down automatically if space for the audit trail is exhausted. (The TOE shall be so configured.) [26.6]	FAU_GEN.1
TF: The audit trail is protected by DAC as part of a trusted subsystem (i.e. auditable events are recorded in the audit trail for all subjects which are to be audited, but no other access to the audit trail is allowed to any but an authorised user) [27.1].	FMT_MTD.1 (3)

Trusted TOE Function	CC SFR
TF: An administrator will be provided with access to the accountability information stored for the purposes of audit [27.2].	FMT_MTD.1 (3)
TF: It is possible for an authorised user to selectively account for the actions of one or more users [28.1].	FAU_SEL.1
TF: Tools exist, and are documented, to examine the accountability configuration files in order that the actions of one or more users be identified selectively [29.1]	FAU_SAR.1, FAU_SAR.3
TF: Tools exist, and are documented, to allow the accountability configuration files to be maintained [29.2].	FAU_SAR.1, FAU_SAR.3
TF: Authorised users will be provided with the ability to statically examine accountability information. [30.1].	FAU_SAR.1, FAU_SAR.3
TF: An authorised user will be able to specify which information is to be extracted from the audit trail [30.2].	FAU_SAR.1, FAU_SAR.3

Table 7: Audit: Mapping between IT Security Functions and SFRs

6.1.6 Object Reuse

The following table maps the trusted TOE functions (TFs) to CC security function requirements (SFRs). The numbering of the TFs implicitly map them to SEFs taken from ITSEC F-B1. TF number [x.y] means TF number y related to SEF x. The SEFs related to Object Reuse are as follows:

SEF31 All storage objects returned to the TOE shall be treated before re-use by other subjects, in such a way that no conclusions can be drawn regarding the preceding content.

Trusted TOE Function	CC SFR
TF: Files are created with zero length. A read from a point beyond the end of the file returns zeroes, whilst a write (the only way of allocating space), only allocates enough space for the data written [31.1].	FDP_RIP.2
TF: FIFOs are created with zero length. A FIFO will only return data written to it since it was created. [31.2].	FDP_RIP.2
TF: All dynamically allocated memory available to a process is cleared on allocation. [31.3].	FDP_RIP.2

Table 8: Object Reuse: Mapping between IT Security Functions and SFRs

6.2 Statement of Assurance Measures

The following table demonstrates the measures the developer has taken to enhance the assurance of the B1/EST-X system and to reach the goal EAL4, by associating the developers measures and EAL4 requirements:

Common Criteria EAL4 requirements	Developer Assurance Measures
Informal TOE security policy model	The developer develops in accordance with well defined procedures following a documented life-cycle model
Security enforcing high-level design	
Descriptive low-level design	
Subset of the implementation of the TSF	
Fully defined external interfaces	
Informal correspondence demonstration	
developer defined life-cycle model	
Well defined development tools	
Functional testing	The developer has a tool-based, automated test system in place
Analysis of coverage	
Testing high-level design	
Independent testing - sample	
Validation of analysis	The developer performed a vulnerability analysis and provided the documentation of the vulnerability analysis
Strength of TOE security function evaluation	
Independent vulnerability analysis	
Partial CM automation, Generation support and acceptance procedures	The developer has installed a quality assurance system requiring configuration control. The developer has a thorough tool supported configuration management in place ensuring a high quality of the TOE and preventing unauthorized changes to the TOE.
Problem tracking CM coverage	The developer has installed a tool based flaw reporting system.
Identification of security measures	The developers site is well protected. The TOE is protected adequately within the configuration control

Common Criteria EAL4 requirements	Developer Assurance Measures
	system.
User guidance	B1/EST-X is released with very detailed user documentation specifically addressing security aspects.
Administrator guidance	B1/EST-X is released with very detailed administrator documentation specifically addressing security aspects.
Delivery Procedures	The developer's delivery procedures are clearly defined and documented.
Installation, generation, and start-up procedures	These topics are addressed specifically in the administration documentation.

Table 9: Statement of Assurance Measures

7 ST Rationale

7.1 Security Objectives Rationale

The following table shows that each security objective addresses at least one threat or assumption:

Objectives	**Threats, Assumptions**
O.I&A: The TOE must uniquely identify all users, and must authenticate the claimed identify before granting a user access to the TOE facilities.	T.IA-1 through T.IA-4, A.TERM
O.DAC: The TOE must provide its users with the means of controlling access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users, and in accordance with the set of DAC rules.	T.AC-5 through T.AC-7, T.OR-1
O.MAC: The TOE must protect the confidentiality of information it is responsible for managing, in accordance with the MAC rules, based directly on comparison of an individual's clearance or authorisation for the information, and the sensitivity designation of the information.	T.AC-1 through T.AC-4, T.OR-1, A.MAC
O.LABEL: The TOE must store and preserve the integrity of sensitivity labels for	T.AC-8 through T.AC-10

information it stores and processes. Data output (exported) by the TOE must have sensitivity labels that are an accurate representation of the corresponding internal sensitivity labels.	
O.AUDIT: The TOE must provide the means of recording any security relevant events, so that an administrator can detect potential attacks or misconfiguration of the TOE security features that would leave the TOE susceptible to attack, and also hold users accountable for any actions they perform that are relevant to security.	T.AA-1, T.AA-2, A.AUDIT
O.INSTALL: Those responsible for the TOE must ensure that the TOE is delivered and installed in a manner which maintains IT security.	T.INSTALL, A.MANAGE, A.NO_EVIL
O.MANAGE: Those responsible for the TOE must ensure that it is managed, administered and operated in a manner which maintains IT security.	T.OPERATE, T.PHYSICAL, A.MANAGE, A.NO_EVIL
O.PHYSICAL: Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack which might compromise IT security.	T.PHYSICAL, A.LOCATE, A.PROTECT
O.CREDEN: Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which maintains IT security.	T.OPERATE, A.ACCESS
O.CONN: Those responsible for the TOE must ensure that no connections to outside systems or users can undermine the IT security objectives.	T.OPERATE, A.PEER, A.CONNECT

Table 10: Mapping Objectives to Threats and Assumptions

The following table shows that each threat and assumption is addressed at least by one security objective:

Threats, Assumptions	**Objectives**
T.IA-1 through T.IA-4	O.I&A
T.AC-5 through T.AC-7	O.DAC
T.AC-1 through T.AC-4	O.MAC
T.AC-8 through T.AC-10	O.LABEL
T.AA-1, T.AA-2	O.AUDIT

T.OR-1	O.DAC, O.MAC
T.INSTALL	O.INSTALL
T.OPERATE	O.MANAGE, O.CREDEN, O.CONN
T.PHYSICAL	O.MANAGE, O.PHYSICAL
A.LOCATE,	O.PHYSICAL
A.PROTECT	O.PHYSICAL
A.ACCESS	O.CREDEN
A.PEER	O.CONN
A.CONNECT	O.CONN
A.TERM	O.I&A
A.MAC	O.MAC
A.AUDIT	O.AUDIT
A.MANAGE	O.INSTALL, O.MANAGE
A.NO_EVIL	O.INSTALL, O.MANAGE

Table 11: Mapping Threats and Assumptions to Objectives

7.2 Security Requirements Rationale

7.2.1 Satisfaction of Security Objectives

The following table shows that each security objective related to IT requirements is addressed by at least one Security Function Requirement:

Objectives	**SFRs**
O.I&A	FIA_UID.2, FIA_UAU.2, FAU_GEN.1, FMT_MTD.1 (1), FMT_SMR.1, FIA_USB.1, FIA_ATD.1, FMT_MTD.1 (2)
O.DAC	FDP_ACC.1, FDP_ACF.1, FMT_MSA.3, FMT_MSA.1 (1), FDP_RIP.2
O.MAC	FDP_IFC.1, FMT_MSA.3 (2), FDP_IFF.2, FDP_RIP.2
O.LABEL	FDP_ITC.1, FDP_ITC.2, FDP_ETC.1, FDP_ETC.2, FMT_MSA.1 (2), FDP_IFF.2
O.AUDIT	FAU_GEN.1, FPT_STM.1, FAU_GEN.2, FMT_MTD.1 (3), FAU_SEL.1, FAU_SAR.1, FAU_SAR.3

Table 12: Mapping Objectives to SFRs

The following table shows that each Security Function Requirement can be related at least to one IT security objective:

SFRs	Objectives
FIA_UID.2	O.I&A
FIA_UAU.2	O.I&A
FMT_MTD.1 (1)	O.I&A
FMT_SMR.1	O.I&A
FIA_USB.1	O.I&A
FIA_ATD.1	O.I&A
FMT_MTD.1 (2)	O.I&A
FDP_ACC.1	O.DAC
FDP_ACF.1	O.DAC
FMT_MSA.3 (1)	O.DAC
FMT_MSA.1 (1)	O.DAC
FDP_RIP.2	O.DAC, O.MAC
FDP_IFC.1	O.MAC
FMT_MSA.3 (2)	O.MAC
FDP_IFF.2	O.MAC, O.LABEL
FDP_ITC.1	O.LABEL
FDP_ITC.2	O.LABEL
FDP_ETC.1	O.LABEL
FDP_ETC.2	O.LABEL
FMT_MSA.1 (2)	O.LABEL
FAU_GEN.1	O.I&A, O.AUDIT
FPT_STM.1	O.AUDIT
FAU_GEN.2	O.AUDIT
FMT_MTD.1 (3)	O.AUDIT
FAU_SEL.1	O.AUDIT
FAU_SAR.1	O.AUDIT
FAU_SAR.3	O.AUDIT

Table 13: Mapping SFRs to Objectives

7.2.2 Suitability of Assurance Requirements

Assurance Level EAL4 provides a known set of mutually supportive and internally consistent assurance components, for which all assurance dependencies are satisfied. This level of assurance is appropriate, because EAL4 provides the necessary confidence

to the evaluators that the TOE can be used to protect classified data and is also achievable by standard industrial development means.

This level is augmented with requirements ALC_FLR.2 (Flaw Reporting Procedures) and ADO_DEL.1 (Delivery Procedures) in order to ensure the secure delivery to the customer and the continuos security maintenance of the product.

7.2.3 Suitability of Strength of Function Claims

The minimum claimed strength of function of high is not in conflict with any of the security objectives or the statements about the security environment. Although a minimum strength of function of medium would also fit, the mechanism of I&A that has to be considered (because it is the only probabilistic mechanism) provides many features that strengthen this mechanism justifying a high rating. This rating also has been applied to AIX 4.3 in a former ITSEC evaluation.

7.2.4 Satisfaction of Dependencies

The following table shows the satisfaction of the dependencies between SFRs as required by the CC:

SFR #	SFRs	Dependencies and Reference
SFR1	FIA_UID.2	no dependencies
SFR2	FIA_UAU.2	FIA_UID.1 (SFR1)
SFR3	FMT_MTD.1 (1)	FMT_SMR.1 (SFR4)
SFR4	FMT_SMR.1	FIA_UID.1 (SFR1)
SFR5	FIA_USB.1	FIA_ATD.1 (SFR6)
SFR6	FIA_ATD.1	no dependencies
SFR7	FMT_MTD.1 (2)	FMT_SMR.1 (SFR4)
SFR8	FDP_ACC.1	FDP_ACF.1 (SFR9)
SFR9	FDP_ACF.1	FDP_ACC.1 (SFR8), FMT_MSA.3 (1) (SFR10)
SFR10	FMT_MSA.3 (1)	FMT_MSA.1 (1) (SFR11), FMT_SMR.1 (SFR4)
SFR11	FMT_MSA.1 (1)	FDP_ACC.1 (SFR8), FMT_SMR.1 (SFR4)
SFR12	FDP_RIP.2	no dependencies
SFR13	FDP_IFC.1	FDP_IFF.1 (SFR15)
SFR14	FMT_MSA.3 (2)	FMT_MSA.1 (2) (SFR20), FMT_SMR.1 (SFR4)
SFR15	FDP_IFF.2	FDP_IFC.1 (SFR13), FMT_MSA.3 (2) (SFR14)
SFR16	FDP_ITC.1	FDP_IFC.1 (SFR13), FMT_MSA.3 (2) (SFR14)
SFR17	FDP_ITC.2	FDP_IFC.1 (SFR13), [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], FPT_TDC.1 Inter-TSF basic TSF data consistency (not satisfied!)
SFR18	FDP_ETC.1	FDP_IFC.1 (SFR13)

SFR #	SFRs	Dependencies and Reference
SFR19	FDP_ETC.2	FDP_IFC.1 (SFR13)
SFR20	FMT_MSA.1 (2)	FDP_IFC.1 (SFR13), FMT_SMR.1 (SFR4)
SFR21	FAU_GEN.1	FPT_STM.1 (SFR22)
SFR22	FPT_STM.1	no dependencies
SFR23	FAU_GEN.2	FAU_GEN.1 (SFR21), FIA_UID.1 (SFR1)
SFR24	FMT_MTD.1 (3)	FMT_SMR.1 (SFR4)
SFR25	FAU_SEL.1	FAU_GEN.1 (SFR21), FMT_MTD.1 (3) (SFR24)
SFR26	FAU_SAR.1	FAU_GEN.1 (SFR21)
SFR27	FAU_SAR.3	FAU_SAR.1 (SFR26)

Table 14: Mapping SFRs to Objectives

The table shows that there is one case where the dependencies are not satisfied, namely SFR17, FDP_ITC.2 depends according to the CC on

- [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], and
- FPT_TDC.1 Inter-TSF basic TSF data consistency

The first requirement shall provide a secured communication channel between the TSF and a user (FTP_TRP.1) or another remote IT product (FTP_ITC.1).

The second requirement shall ensure that the interpretation of the label information during import from *another trusted IT-product* are interpreted in a consistent way.

The intention of these requirements is to receive and interpret the label information correctly during import of data. The TOE ensures this intention by providing one specific tool (*lpax*) to export and import labeled information on tape or disk, that enforces the correct interpretation of labels. So while the wording of the two CC requirements does not fit for *lpax* the intention is met by the tool's functionality.

This is reflected by adding an additional rule under FDP_ITC.2.5:

> The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC:
>
> > *For multi-level channels it shall be ensured by the communication protocol that the recipient can completely and unambiguously reconstruct and pair the received data and attributes. (By "communication protocol" is meant the data and label encoding used by the import/export utility).*

Therefore there is no flaw in the binding of the TOE's functionality.

7.2.5 Mutual Support of Security Requirements

The dependency analysis in chapter 7.2.4 "Satisfaction of Dependencies" above shows that the binding between the SFRs is complete. There are no additional functional requirements needed to support the implemented one. This is also supported by the fact

that the stated SFRs reflect the functionality class F-B1 from [ITSEC] which is established as a well-known, well binding set of security functions.

7.3 TOE Summary Specification Rationale

7.3.1 Satisfaction of SFRs

The tables in the subsections of section 5.1 "TOE Security Functional Requirements" show that each of the TOE IT security functions map to at least one SFR.

The reverse mapping showing that each SFR is mapped at least onto one IT security function is provided in the following table:

SFRs	**IT security functions**
FIA_UID.2	TF [1.1], TF [1.4], TF [2.3]
FIA_UAU.2	TF [1.1], TF [1.3], TF [1.4], TF [2.1], TF [2.3]
FMT_MTD.1 (1)	TF [1.2], TF [1.5], TF [1.7], TF [1.8], TF [1.9],TF [2.3], TF [3.1], TF [3.2]
FMT_SMR.1	TF [1.7], TF [3.1], TF [3.3], TF [4.2], TF [10.1], TF [10.2]
FIA_USB.1	TF [4.1]
FIA_ATD.1	TF [4.1]
FMT_MTD.1 (2)	TF [2.2], TF [4.2], TF [10.1], TF [10.2]
FDP_ACC.1	TF [5.1], TF [5.5], TF [5.6], TF [7.1]
FDP_ACF.1	TF [5.1], TF [5.4], TF [5.5], TF [5.6], TF [5.7], TF [7.1], TF [7.2], TF [23.1], TF [25.1]
FMT_MSA.3 (1)	TF [5.2]
FMT_MSA.1 (1)	TF [5.3],TF [8.1], TF [9.1]
FDP_RIP.2	TF [31.1], TF [31.2], TF [31.3]
FDP_IFC.1	TF [11.1], TF [11.2], TF [14.1]
FMT_MSA.3 (2)	TF [11.3], TF [11.4]
FDP_IFF.2	TF [11.5], TF [11.6], TF [12.1], TF [12.2], TF [12.3], TF [12.4], TF [12.5], TF [12.6], TF [14.1], TF [15.1], TF [17.4], TF [17.5], TF [25.1]
FDP_ITC.1	TF [16.1], TF [17.1]
FDP_ITC.2	TF [13.1], TF [17.1], TF [17.2], TF [19.1], TF [19.2], TF [19.3]
FDP_ETC.1	TF [17.1]
FDP_ETC.2	TF [13.1], TF [17.1], TF [17.2], TF [19.1], TF [19.2], TF [19.3], TF [21.1], TF [21.2]
FMT_MSA.1 (2)	TF [17.3], TF [20.3]
FAU_GEN.1	TF [1.6], TF [26.1], TF [26.2], TF [26.3], TF [26.6]

SFRs	IT security functions
FPT_STM.1	TF [26.1]
FAU_GEN.2	TF [26.3]
FMT_MTD.1 (3)	TF [26.4], TF [27.1], TF [27.2]
FAU_SEL.1	TF [28.1]
FAU_SAR.1	TF [29.1], TF [29.2], TF [30.1], TF [30.2]
FAU_SAR.3	TF [29.1], TF [29.2], TF [30.1], TF [30.2]

Table 15: Mapping SFRs to IT Security Functions

7.3.2 Mutual Support of IT Security Functions

The section 7.2.5 "Mutual Support of Security Requirements" above shows that the SFRs are mutually supportive. As 7.3.1 "Satisfaction of SFRs" shows, there is a complete mapping between SFRs and IT security functions. Therefore the IT security functions are also mutually supportive. This fact is also supported by the fact that the IT security functions of the TOE reflect the functionality class F-B1 from [ITSEC] which is established as a well-known, well binding set of functions.

Additionally the Binding Analysis [BIND] shows that the IT security functions provide a mutually supportive whole with more detail.

7.3.3 Satisfaction of Assurance Requirements by Assurance Measures

The table provided in chapter 6.2 "Statement of Assurance Measures" already maps the CC assurance requirements to the assurance measures taken by the developer, showing that each of the assurance requirements are addressed by the developer.

8 References

[ITSEC] Information Technology Security Evaluation Criteria (ITSEC) Provisional Harmonised Criteria of France, Germany, the Netherlands and the United Kingdom Version 1.2, June 1991

[CC20] Common Criteria Version 2.0

[BXOLD41222508] B1/EST-X Binding Analysis, 41222508, Rev. 1.1

[SRB431] Software Release Bulletin for 2.0.1.0 - October 5, 1998