HITACHI
Inspire the Next

Hitachi ID Systems, Inc.

Hitachi ID Management Suite

Version 3.2 Security Target (EAL2)
Version 1.98

Hitachi ID Systems, Inc.

Document name:	....	Version 3.2 Security Target (EAL2)
Submitted to:	....	DOMUS IT Security Laboratory Attn:
Submitted by:	....	Hitachi ID Systems, Inc.
Document date:	....	April 21, 2008
Document path:	....	PRCS:qa/ccc/doc/st-new.tex

Revision History

Rev. #	Description	By	Date of Issue
1.0	Initial draft	Enzo Bertorelli	26-Aug-2004
1.1	Update SFR list	Enzo Bertorelli	31-Aug-2004
1.2	Update Functional Characteristics	Enzo Bertorelli	13-Sep-2004
1.3	Update Detailed description	Enzo Bertorelli	15-Sep-2004
1.4	Minors updates to all sections as per DOMUS review	Enzo Bertorelli	27-Oct-2004
1.5	Updates to diagrams in section 1. Updates to the SFR descriptions. Updates to correlations section.	Enzo Bertorelli	15-Nov-2004
1.6	Corrections from Hitachi ID feedback	Enzo Bertorelli	25-Nov-2004
1.7	Changes made as result of CSE suggestions	Enzo Bertorelli	07-Jan-2005
1.8	General Revision	Luc D. Cousineau	18-Apr-2005
1.9	Changes to address DOMUS OR 01	Enzo Bertorelli, Luc D. Cousineau	16-Sep-2005
1.91	Changes to address CB OR 01	Luc D. Cousineau	27-Nov-2005
1.92	Final Draft	Stacey Kaluta	23-June-2006
1.93	Minor revision to Final Draft	Stacey Kaluta	16-Aug-2006
1.94	Minor revision to Final Draft to address OR8	Stacey Kaluta	14-Feb-2008
1.95	Updated conventions and terminology	Stacey Kaluta	27-Mar-2008
1.96	Further updates to acronyms and abbreviations	Stacey Kaluta	03-Apr-2008
1.97	Removed “confidential information” and associated text from control page	Stacey Kaluta	04-Apr-2008
1.98	Rebranding from M-Tech to Hitachi ID	Stacey Kaluta	08-APR-2008

Table of Contents

List of Tables

List of Figures

Conventions and Terminology

Through this document, operations performed in Common Criteria requirements are highlighted *like this*.

Acronyms and abbreviations

CC	Common Criteria
CCCS	Canadian Common Criteria Scheme
CEM	Common Methodology for Information Technology Security
COTS	Commercial-Off-The-Shelf
EAL	Evaluation Assurance Level
PP	Protection Profile
SARs	Security Assurance Requirements
SFP	Security Function Policy
SFRs	Security Functional Requirements
ST	Security Target
TBD	To Be Determined
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy

Document Organization

Section 1 provides the introductory material for the Security Target.

Section 2 provides general purpose and TOE description.

Section 3 provides a discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware or software or through the environmental controls.

Section 4 defines the security objectives for both the TOE and the TOE environment.

Section 5 contains the functional and assurance requirements derived from the Common Criteria Parts 2 and 3, respectively, that must be satisfied by the TOE.

Section 6 describes the details specific to the TOE implementation of the security measures described in this document.

Section 7 contains the claims of Protection Profile conformance for this Security Target.

Section 8 provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective.

1 Introduction

This section identifies the Security Target and Target of Evaluation (TOE) identification, ST conventions, and ST conformance claims. This ST describes a set of security requirements and specifications to be used as the basis for evaluation of an identified Information Technology (IT) product.

The IT product described in this ST is the Hitachi ID Management Suite Version 3.2 software, developed by Hitachi ID Systems, Inc. Throughout this document, the TOE will be referred to as the ID Management Suite. The ID Management Suite is composed of 2 components: P-Synch and ID-Synch. The ID Management Suite software components are the subject of the evaluation and are called the Target of Evaluation (TOE).

Note: The *Hitachi ID Management Suite* was previously known as the *M-Tech Identity Management Suite. Hitachi ID Systems, Inc.* was previously known as *M-Tech Information Technology, Inc.*

M-Tech was acquired by Hitachi, Ltd. In April of 2008.

1.1 Identification

Title:	Hitachi ID Management Suite Version 3.2 Security Target (EAL2)
ST Version:	1.98
TOE Identification:	Hitachi ID Management Suite Version 3.2
Authors:	Enzo Bertorelli, Luc D. Cousineau, Stacey Kaluta
CC Version:	2.2
Keywords:	Commercial-off-the-shelf (COTS), identity management, password management, identification, authentication, networked information systems.

1.2 Security target overview

Hitachi ID's ID Management Suite is made up of 2 major components:

- **ID-Synch** which provides identity management across multiple platforms, both current and legacy.
- **P-Synch** which provides automated Enterprise password management on a self serve basis. These can include password synchronization and password reset. This framework provides a uniform password policy throughout the Enterprise and provides strong data encryption.

These two components make up the entire TOE for this security Target (ST). Its security characteristics are described below as is the boundary of this evaluation.

The Common Criteria (CC) Evaluation Assurance Level 2 evaluation documented herein describes the assumptions, threats, security objectives that pertain to the product in its normal use and presents findings that establish its functional properties at that level.

This documentation presents the rationale that the evaluation criteria presented are consistent and complete, and that the functional and assurance requirements cited are fulfilled.

Throughout this document, we will refer to “P-Synch Protected User Record Access Control” to refer to the access control policy enforced by the P-Synch component of the ID Management Suite and “ID-Synch Protected User Record Access Control” to refer to the access control policy enforced by the ID-Synch component of the ID Management Suite. Wherever we refer to “Protected User Record Access Control”, we will be referring to the combination of the “P-Synch protected User Record Access Control” and “ID-Synch protected User Record Access Control” policies.

1.3 CC conformance claim

The ID Management Suite is conformant to Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements (Version 2.2, January 2004) Extended (with FAU_ADG.1). All International Common Criteria Interpretations through September, 2004 have been applied.

The ID Management Suite is conformant to Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements (Version 2.2, January 2004). All International Common Criteria Interpretations through September, 2004 have been applied.

The ID Management Suite is being evaluated to Evaluation Assurance Level 2 (EAL2) under the Canadian Common Criteria Scheme (CCCS) using the Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 2.2, January 2004. All International Common Criteria Interpretations through September, 2004 have been applied.

2 TOE Description

The ID Management Suite is a complete identity management solution enabling organizations to securely organize and manage user identities across enterprise applications and systems.

The ID Management Suite combines the power of Hitachi ID's flagship technologies, ID-Synch for user provisioning and P-Synch for password management.

The following sections describe the ID Management Suite and its components.

2.1 ID-Synch

ID-Synch is a complete user provisioning solution that automates and simplifies the routine tasks of managing users across multiple systems. Enterprise-scale organizations depend on ID-Synch to ensure that their employees and contractors are securely and efficiently connected to vital systems and information.

ID-Synch strengthens security by:

- Providing consolidated reports on user access to systems that can be used to review compliance with security policy
- Enforcing authorization rules over change requests
- Implementing standards over the setup of new login IDs
- Applying access controls to security administrators
- Providing an audit log of all provisioning / deprovisioning events

2.1.1 Primitive operations

ID-Synch primitive operations, which create or modify user objects on managed systems, may be any of the following:

- Create new and delete existing accounts for a user
- Check enabled / disabled status of existing accounts
- Set enabled / disabled status of existing accounts
- Read attributes of existing user accounts
- Set attributes of existing user accounts
- Modify the membership of existing accounts in security groups
- Change the context of a user in a structured directory

2.1.2 Core features

ID-Synch core features include:

Consolidated user administration

Security administrators can log into an ID-Synch web user interface, from which they can: create new accounts; delete, enable, disable, or update existing accounts; and manage the membership of users in security groups and distribution lists.

Simplified management of users across systems reduces the workload for security administrators.

Self-service user administration workflow

Users are empowered to submit requests for new, changed or terminated systems access or to change their personal profile information. For example, a manager may submit a request for new accounts for a new hire or contractors may request additional system access for themselves.

Requests are automatically validated, filled out with extra attributes such as login ID or directory OU and routed to the appropriate authorizers. Authorizers are assigned based on the resources requested or the identity of the requester. Authorizers review open requests and may approve or reject them. Approved requests are automatically applied to managed systems by ID-Synch.

In many organizations, most of the cost and delay of access management is due to entry, routing and approvals of change requests. ID-Synch streamlines requests with easy input and parallel routing, to significantly reduce the delay between first input of a request and its fulfillment.

Rapid access provisioning improves user productivity: new hires no longer spend days or weeks waiting for access before they can start work. Managers spend less time filling in and tracking paper requests.

2.2 P-Synch

P-Synch helps organizations manage passwords and other forms of authentication more effectively to reduce IT support costs, increase productivity and enhance corporate security.

P-Synch strengthens security by providing:

- A strong enterprise-wide password policy enforcement facility
- Effective user authentication, especially for self-service and assisted password resets
- Password synchronization to help users remember, rather than write down, their passwords
- The ability to securely delegate the right to reset passwords to front-line support staff
- Accountability for password resets
- Encryption of all transmitted passwords

2.2.1 Primitive operations

P-Synch primitive operations may be any of the following:

- Set / reset passwords
- Clear intruder lockout flags on systems that support intruder lockout
- Set account enabled status on systems that support enable / disable
- Update password expiry information

2.2.2 Core features

P-Synch core features include:

Assisted password reset

Authorized support analysts can log into a P-Synch web user interface, look up a caller's profile, authenticate the caller by keying in answers to personal questions, and reset one or more passwords. A closed ticket can be automatically written to the call tracking system.

Support staff do not require any privileges to systems on which P-Synch allows them to reset passwords.

Self-service password reset

A user who has forgotten his password or triggered an intruder lockout can log into P-Synch, from his own computers or that of a neighbor, with another form of authentication to perform self-service password reset. Supported authentication factors include answering personal questions in the form of Q&A, using a hardware token (SecurID, SafeWord), using a biometric sample, and smart cards.

Automated password reset allows locked out users to reset their own passwords, effectively addressing the problem of forgotten passwords. P-Synch creates a secure and efficient process for users to reset their passwords, thus minimizing the help desk call volume and time spent with the help desk resetting the passwords.

Once authenticated, users can reset their own passwords without calling the help desk. Tickets can be automatically created on a call tracking system.

Web-based password synchronization

Users can synchronize some or all of their passwords by using a P-Synch web interface to make routine password changes. The password policy is clearly stated on the screen and enforced immediately. Each system where the user has a login ID is represented by a name and a check box.

Transparent password synchronization

When users change their Windows NT, Active Directory, LDAP (Sun, IBM), Unix, OS/390, and OS/400 password, the new password is subjected to a global password policy in addition to the native policy. If the password is acceptable, the new password is changed both on the initial system and, automatically, on every other system where the user has a login ID.

Password policy enforcement

P-Synch enforces a uniform, global policy in addition to the various password policies enforced natively on each managed system.

The built-in password policy engine includes over 50 standard rules, plus a regular expression engine and plug-in system, allowing organizations to define new rules. Open-ended password history and dictionary checks are included.

2.3 Shared architecture

P-Synch and ID-Synch use the same product architecture for:

2.3.1 Security

The ID Management Suite offers multi-layered security. This includes running on a hardened OS, using file system ACLs, providing strong application-level user authentication, encrypting sensitive data, enforcing application-level ACLs, and storing log data indefinitely.

2.3.2 Interaction with target systems

The ID Management Suite server interacts with target systems (managed systems) using native communication protocols wherever possible. This minimizes the amount of software that must be installed on managed systems. For those systems where a secure remote administration facility is not available, a combination of server-side software and scripting technologies are used. This is illustrated in Figure 1.

Some of the supported target systems include: Active Directory, LDAP directories, Windows NT servers / domains, Novell NDS, Unix (various flavors), OS/400, OS/390, DB2 database, Oracle database, Sybase database, MSSQL database, SAP, PeopleSoft, Exchange, GroupWise, Notes / Domino, Telnet sessions, Windows command-line integration, web forms, web services (SOAP, XML), and SecurID tokens.

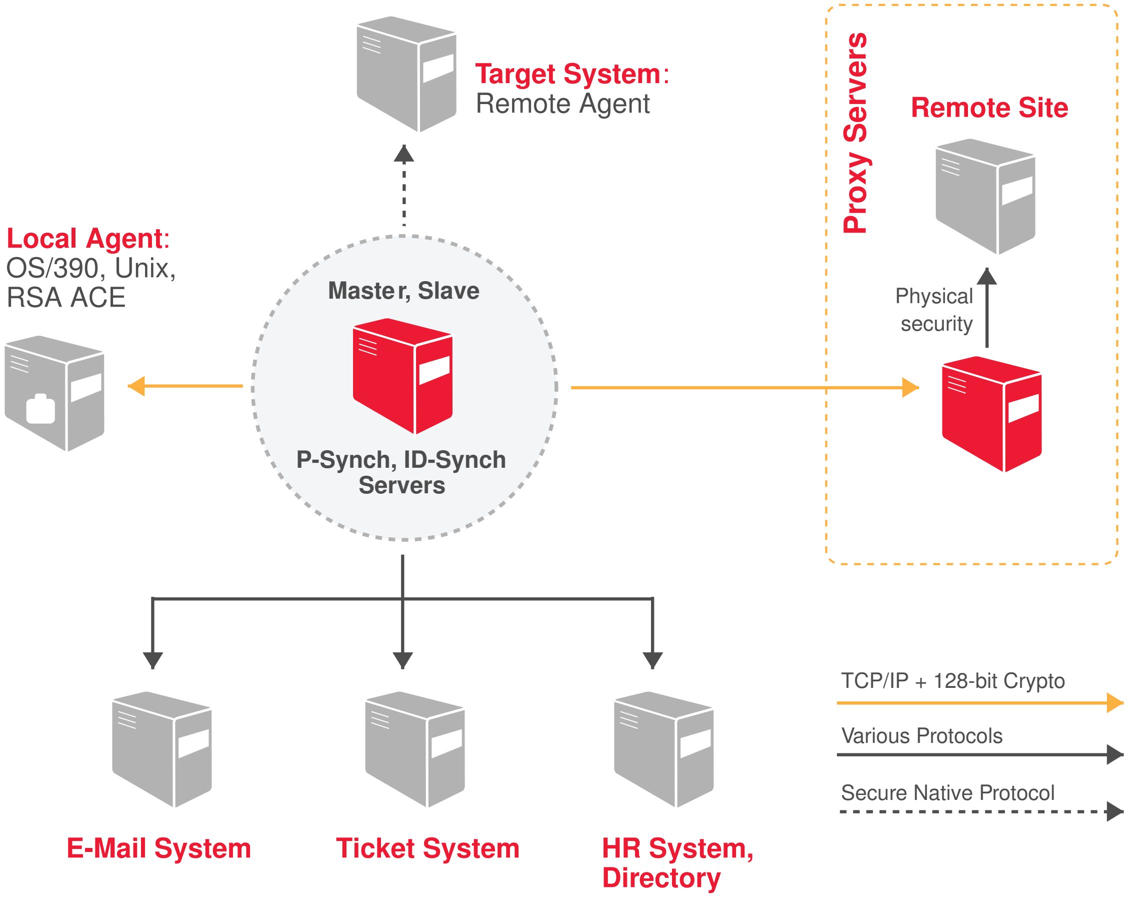

Figure 1: Integration With Target Systems

2.3.3 Web access

Most ID Management Suite functions are accessed using a web browser. The ID Management Suite user interface is primarily HTML and works with most web browsers. In particular, since the web interface does not require active content (ActiveX), it works with older browsers, locked down browsers, and through filtering firewalls.

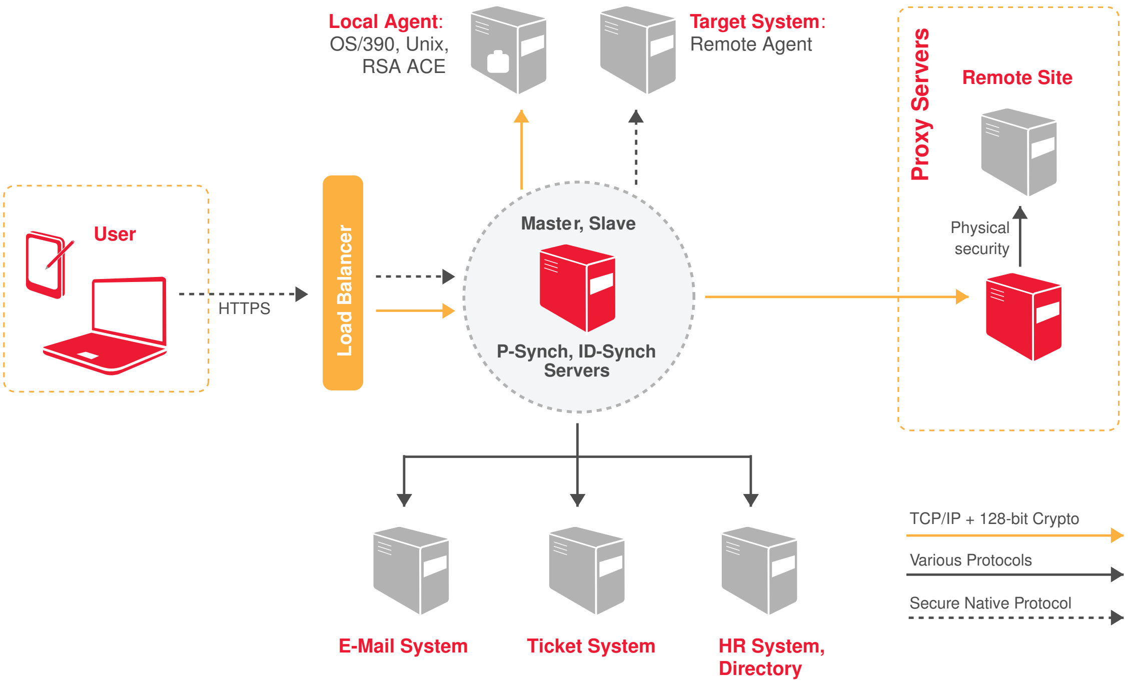

Figure 2: Web access architecture diagram

For added security, the web server software on the ID Management Suite server can be configured to use HTTPS. To enable encryption between users' web browsers and the ID Management Suite interface, an organization purchases (from a certificate authority) or generates its own digital server certificate and installs it for the web site. This is no different from any other secure web application (web banking, e-Commerce).

2.4 TOE boundary

For the purposes of this security target, the TOE boundary includes Hitachi ID's ID Management Suite software, as well as P-Synch/390 – a proprietary started task and security exit – to be used as local agent installed on the IBM OS/390 operating system.

Note: Although other platforms exist (see subsubsection 2.3.2 on Page 8) they are not within the TOE boundary as their interface functions are handled by native methods (APIs or the underlying OS).

The following diagram describes the relationships within the TOE:

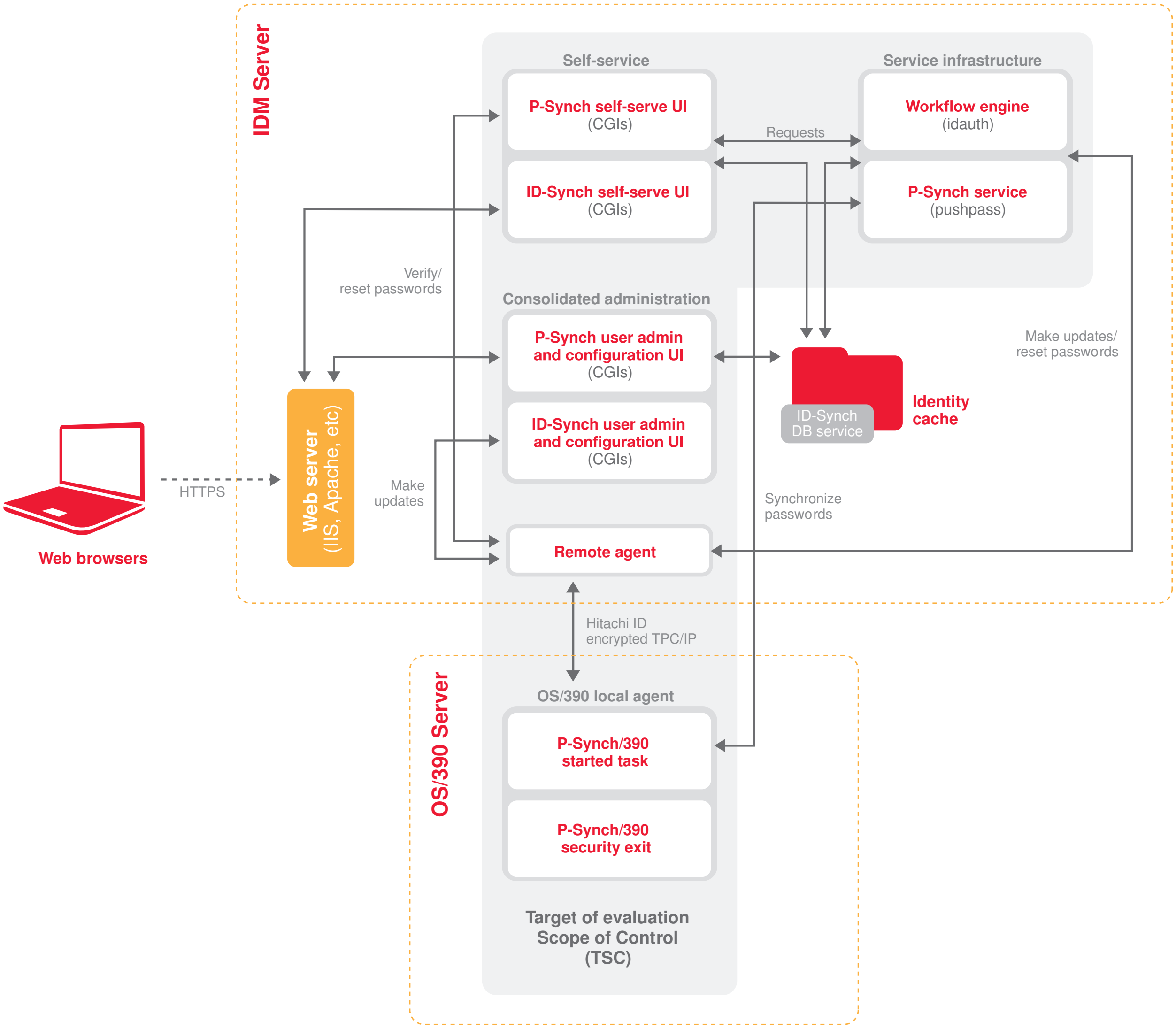

Figure 3: TOE Boundary

Note: The TOE is constituted of the modules within the highlighted (gold) area. The name of the physical processes providing the services is indicated in brackets after the service description. There are no hardware or firmware components within the TOE boundary.

3 TOE Security Environment

The TOE security environment consists of the threats to security, organizational security policies, and usage assumptions as they relate to the TOE.

The ID Management Suite provides for a level of protection that is appropriate for IT environments that require a harmonized password policy across an enterprise. The software is not designed to withstand physical attacks directed at disabling or bypassing its security features, however it is designed to withstand some logical attacks originating from its attached network.

Threats are undesirable events and are characterized in terms of a threat agent, a presumed attack method, vulnerabilities that are the foundation for the attack, and identification of the asset under attack.

Threat agents are subjects which have not been granted authorized access to the assets. Assets comprise the TOE and the authentication data held by the TOE on behalf of authorized users.

For this evaluation, the threat agents are assumed to have an attack potential of low. As a result, the TOE has been developed with the assumption that a potential attacker would have a proficient level of expertise, access to public knowledge of the TOE, restricted access to the TOE, and have access to standard equipment.

3.1 Secure usage assumptions

A.Competent_Admin — Competent system administrators

System administrators are competent to manage the TOE and the security of the information it contains. The administrators will not compromise the security of the TOE or its data either willfully or by neglect.

A.Coop_User — Cooperative users

Users cooperate with those responsible for managing the TOE to maintain TOE security and will follow all directives and prescriptions imposed by the administrators and / or guidance provided with the TOE.

A.Environment — Secure Environment

The environment is secure and the administrators have a good working knowledge and know how to manage the OS underlying the TOE.

A.Network — Secure Network

Network connected to the TOE is protected from active attacks (i.e. data mode intrusion).

A.Physical

Physical Security

TOE is physically secure. The TOE will be deployed in an environment providing physical security adequate to protect against unauthorized access.

A.Ext_Services

External Services

In cases where external services (e.g. IVR) are used, the services are secure and do not offer unauthorized access to the TOE.

A.Back_End_Auth

Back End Authentication

There is a back-end system handling the authentication of non-administrative users.

A.Time_Source

Reliable Time Source

The TOE's environment provides a reliable time source for time stamping audit records.

A.Reference_Monitor

Reference Mediation

The TOE's environment provides a properly implemented reference monitor and enforces the domain separation required for the application of the TOE's discretionary access control policy.

3.2 Threats to security

T.Disclosure

Unauthorized disclosure of user data.

An attacker may attempt capture the managed data while it is in transit between remote parts of the TOE.

3.3 Organizational security policies

P.Accountability

Individual accountability

Individuals shall be held accountable for their actions.

4 Security Objectives

4.1 Security objectives for the TOE

O.Audit

Auditing

Maintain audit records. Provide individual accountability for audited events. Uniquely identify each user so that auditable actions can be traced to a user.

O.I&A

Identify and authenticate a user to support accountability

Provide the basic I&A functions that will support user accountability.

O.Secure_Transfer

User data is secured from disclosure in transit

User data is secured from disclosure in transit between remote parts of the TOE.

O.User_Defined_AC

User-defined access control

Enforce an access control policy whereby company policies determine who may access the data controlled by the TOE.

4.2 Security objectives for the IT environment

OE.Audit

Audit records with identity

The IT environment provides the date and time components of the audit records.

OE.AC

Environmental access control

The IT environment enforces the reference mediation and domain separation required to implement the access controls.

OE.Back_End_Auth

Back-end Authentication

The IT environment provides the back-end authentication services required to authenticate non-administrative users.

OE.Competent_Admin

Competent system administrators

The IT environment ensures that System administrators are competent to manage the TOE and the security of the information it contains and that the administrators will not compromise the security of the TOE or its data either willfully or by neglect.

OE.Coop_User

Cooperative users

The IT environment ensures that users cooperate with those responsible for managing the TOE to maintain TOE security and will follow all directives and prescriptions imposed by the administrators and / or guidance provided with the TOE.

OE.Environment Secure Environment

The IT environment must ensure that the TOE is secure and the administrators have a good working knowledge and know how to manage the OS underlying the TOE.

OE.Network Secure Network

The IT environment must ensure that the network connected to the TOE is protected from active attacks (i.e. data mode intrusion).

OE.Physical Physical Security

The IT environment must ensure that the TOE is physically secure.

OE.Ext_Services External Services

In cases where external services (e.g. IVR) are used, the IT environment must ensure that the services are secure and do not offer unauthorized access to the TOE.

5 IT Security Requirements

5.1 TOE security functional requirements

5.1.1 Security audit **(FAU)**

5.1.1.1 Audit data generation (FAU_ADG.1)

The TSF shall be able to generate an audit record of the following auditable event:

a) All auditable events for the *not specified* level of audit; and

b) *Events listed in Table 5-2*. FAU_ADG.1.1

The TSF shall record within each audit record at the following information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, *no other audit relevant information*. FAU_ADG.1.2

Rationale: FAU_ADG.1.1 and FAU_ ADG.1.2 are necessary to specify audit requirements as performed by the TOE. FAU_SAR.1 has a dependency on FAU_GEN.1. FAU_ADG.1.1 which is an extended security requirement based on FAU_GEN.1, generates the audit record and FAU_ADG.1.2 indicates the information contained within the audit record. The dependency is satisfied because a record has to first be generated before it can be read. The TOE audit function does not record start up and shut down of the audit function so the extended requirement is fulfilling the dependency requirement instead of FAU_GEN.1.

Table 5-2 Auditable Events

Component	Audited Events
FDP_ACF.1	All requests to perform an operation on an object covered by the SFP, except special cases where the recording of failure is not required. The identity of the object.
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken. The restoration to normal state.
FIA_SOS.1	Rejection or acceptance by the TSF of any tested secret.
FIA_UAU.2	All use of the authentication mechanism.

. . . continued on the next page

Table 5-2 continued

Component	Audited Events
FIA_UID.2	All use of the user identification mechanism, including the identity provided during successful attempts.
FMT_MSA.1	All modifications of the values of security attributes.
FMT_MSA.3	Modifications of the default setting of permissive or restrictive rules. All modifications of the initial value of security attributes.
FMT_SMR.1	Modifications to the group of users that are part of a role.

5.1.1.2 User identity association (FAU_GEN.2)

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

5.1.1.3 Audit review (FAU_SAR.1)

The TSF shall provide *Administrative users who are authorized to read audit records* with the capability to read *all audit information* from the audit records. FAU_SAR.1.1

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

5.1.1.4 Restricted audit review (FAU_SAR.2)

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

5.1.1.5 Selectable audit review (FAU_SAR.3:P-Synch)

The TSF shall provide the ability to perform *searches* of audit data based on *account name, event type, and / or date*. FAU_SAR.3.1

5.1.1.6 Selectable audit review (FAU_SAR.3:ID-Synch)

The TSF shall provide the ability to perform *searches* of audit data based on *operation, target system, and / or date*. FAU_SAR.3.1

5.1.1.7 Protected audit trail storage (FAU_STG.1)

The TSF shall protect the stored audit record from unauthorized deletion. FAU_STG.1.1

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

5.1.2 User data protection **(FDP)**

5.1.2.1 Subset access control (FDP_ACC.1)

The TSF shall enforce the *Protected User Record Access Control* on:

a) *Subjects: administrative users and regular users of the TOE;*

b) *Objects: global password policy, audit data, user objects, and access control groups*;

c) *Operations: modify global password policy, read TOE audit data, manage (create, update, or delete) user objects, manage (create, update, delete) access control groups, and modify administrative users' passwords*. FDP_ACC.1.1

5.1.2.2 Security attribute based access control (FDP_ACF.1:P-Synch)

The TSF shall enforce the *P-Synch Protected User Record Access Control* to objects based on the following:

a) *The subject attributes: account name, user role, and user rights associated with subjects: administrative users and regular users*.

b) *The following access control attributes associated with the object:*

- ***Global password policy:*** *password policy rules*
- ***Audit data:*** *audit data records*
- ***User objects:*** *account name, user role, user rights, administrative user password, and user profile data*. FDP_ACF.1.1:P-Synch

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

- ***Global password policy:***
  - *Modification of the global password policy is limited to administrative users with the appropriate right*.
- ***Audit data:***
  - *The reading of audit data is limited to administrative users with the appropriate right*.

- ***User objects:***
  - *The management of administrative user objects is limited to administrative users with the appropriate right*.

    Additionally, an administrative user can only manage administrative user objects that have equal or lesser user rights. An administrative user cannot modify his own user rights.
  - *The management of “manually added” regular user objects is limited to administrative users with the appropriate right*. FDP_ACF.1.2:P-Synch

> **Note:** Manually added regular users are those added directly to P-Synch by an administrative user. Unlike other regular users, they are not imported from the IT environment.

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *no additional rules.* FDP_ACF.1.3:P-Synch

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

5.1.2.3 Security attribute based access control (FDP_ACF.1:ID-Synch)

The TSF shall enforce the *ID-Synch Protected User Record Access Control* to objects based on the following:

a) *The subject attributes: account name, user role, user rights, and access control groups associated with subjects: administrative users and regular users*.

b) *The following access control attributes associated with the object:*

- ***Global password policy:*** *password policy rules*
- ***Audit data:*** *audit data records*
- ***Access control group:*** *group members*
- ***User objects:*** *account name, user role, user rights, administrative user password, and user profile data*. FDP_ACF.1.1:ID-Synch

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

- ***Global password policy:***
  - *Modification of the global password policy is limited to administrative users with the appropriate right*.
- ***Audit data:***
  - *The reading of audit data is limited to administrative users with the appropriate right*.
- ***Access control groups:***
  - *The management of access control groups is limited to administrative users with the appropriate rights*.

- ***User objects:***
  - *The management of administrative user objects is limited to administrative users with the appropriate right*.

    Additionally, an administrative user can only manage administrative user objects that have equal or lesser rights. An administrative user cannot modify his own user rights.
  - *The management of "manually added" regular user objects is limited to administrative users with the appropriate right*.

    > **Note:** Manually added regular users are those added directly to ID-Synch by an administrative user. Unlike other regular users, they are not imported from the IT environment and are not created with accounts on target systems.

  - *The management of regular user objects is provided to administrative users with the appropriate right.* FDP_ACF.1.2:ID-Synch

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *no additional rules.* FDP_ACF.1.3:ID-Synch

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

5.1.3 Identification and authentication (FIA)

5.1.3.1 Authentication failure handling (FIA_AFL.1)

The TSF shall detect when *an administrator configurable positive integer within 1-99* unsuccessful authentication attempts occur related to *the unsuccessful authentication attempts since the last successful authentication for the indicated user*. FIA_AFL.1.1

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall *disable the user until unlocked by an administrative user*. FIA_AFL.1.2

> **Note:** An administrative user can also set the number of minutes after which a locked-out user will automatically be re-enabled (the lockout duration). By default, this setting is off.

5.1.3.2 User attribute definition (FIA_ATD.1:P-Synch)

The TSF shall maintain the following list of security attributes belonging to individual users: *account name, user role, user rights, and administrative user password*. FIA_ATD.1.1

5.1.3.3 User attribute definition (FIA_ATD.1:ID-Synch)

The TSF shall maintain the following list of security attributes belonging to individual users: *account name; user role, user rights, access control group, and administrative user password.* FIA_ATD.1.1

5.1.3.4 Verification of secrets (FIA_SOS.1)

The The TSF shall provide a mechanism to verify that secrets meet *SOF-high.* FIA_SOS.1.1

5.1.3.5 User authentication before any action (FIA_UAU.2:Admin)

The TSF shall require each user *belonging to an administrative role* to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. FIA_UAU.2.1:Admin

> **Note:** Regular users are authenticated using a back-end authentication mechanism.

5.1.3.6 Protected authentication feedback (FIA_UAU.7)

The TSF shall provide only *obscured feedback* to the user while the authentication is in progress. FIA_UAU.7.1

5.1.3.7 User identification before any action (FIA_UID.2)

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

5.1.3.8 User-subject binding (FIA_USB.1:P-Synch)

The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: *account name, user role, and user rights*. FIA_USB.1.1

The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: *the user session shall represent the user's access rights predetermined by his role and assigned rights*. FIA_USB.1.2

The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: *no rules*. FIA_USB.1.3

5.1.3.9 User-subject binding (FIA_USB.1:ID-Synch)

The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: *account name, user role, user rights, and access control group*. FIA_USB.1.1

The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: *the user session shall represent the user's access rights predetermined by his role and assigned rights*. FIA_USB.1.2

The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: *no rules*. FIA_USB.1.3

5.1.4 Security management (FMT)

5.1.4.1 Management of security attributes (FMT_MSA.1:P-Synch)

The TSF shall enforce the *P-Synch Protected User Record Access Control* to restrict the ability to *modify* the security attributes *password policy rules* to *administrative users with the appropriate right*.

The TSF shall enforce the *P-Synch Protected User Record Access Control* to restrict the ability to *query* the security attributes *audit data records* to *administrative users with the appropriate right*.

The TSF shall enforce the *P-Synch Protected User Record Access Control* to restrict the ability to *modify* the security attributes *administrative user password* to *administrative users authorized to modify their own passwords, and administrative users authorized to modify other administrative users' passwords.* FMT_MSA.1.1

The TSF shall enforce the *P-Synch Protected User Record Access Control* to restrict the ability to *create* the security attributes *account name* to *administrative users authorized to do so*. FMT_MSA.1.1

The TSF shall enforce the *P-Synch Protected User Record Access Control* to restrict the ability to *modify* the security attributes *user rights* to *administrative users authorized to do so*. FMT_MSA.1.1

The TSF shall enforce the *P-Synch Protected User Record Access Control* to restrict the ability to *modify* the security attributes *user profile data* to *administrative users authorized to do so*. FMT_MSA.1.1

The TSF shall enforce the *P-Synch Protected User Record Access Control* to restrict the ability to *assign* the security attributes *user role* to *administrative users authorized to do so*. FMT_MSA.1.1

5.1.4.2 Management of security attributes (FMT_MSA.1:ID-Synch)

The TSF shall enforce the *ID-Synch Protected User Record Access Control* to restrict the ability to *modify* the security attributes *password policy rules* to *administrative users with the appropriate right*.

The TSF shall enforce the *ID-Synch Protected User Record Access Control* to restrict the ability to *query* the security attributes *audit data records* to *administrative users with the appropriate right*.

The TSF shall enforce the *ID-Synch Protected User Record Access Control* to restrict the ability to *modify* the security attributes *administrative user password* to *administrative users authorized to modify their own passwords, and administrative users authorized to modify other administrative users' passwords*. FMT_MSA.1.1

The TSF shall enforce the *ID-Synch Protected User Record Access Control* to restrict the ability to *create* the security attributes *account name* to *administrative users and regular users authorized to do so*. FMT_MSA.1.1

The TSF shall enforce the *ID-Synch Protected User Record Access Control* to restrict the ability to *modify* the security attributes *user rights* to *administrative users authorized to do so*. FMT_MSA.1.1

The TSF shall enforce the *ID-Synch Protected User Record Access Control* to restrict the ability to *modify* the security attributes *user profile data* to *administrative users authorized to do so*. FMT_MSA.1.1

The TSF shall enforce the *ID-Synch Protected User Record Access Control* to restrict the ability to *manage* the security attributes *group members* to *administrative users authorized to do so*. FMT_MSA.1.1

The TSF shall enforce the *ID-Synch Protected User Record Access Control* to restrict the ability to *assign* the security attributes *user role* to *administrative users authorized to do so*. FMT_MSA.1.1

5.1.4.3 Static attribute initialization (FMT_MSA.3)

The TSF shall enforce the *Protected User Record Access Control* to provide *restrictive* default values for security attributes that are used to enforce the SFP. FMT_MSA.3.1

The TSF shall allow the *administrative users and regular users with the required rights* to specify alternative initial values to override the default values when an object or information is created. FMT_MSA.3.2

5.1.4.4 Specification of Management Functions (FMT_SMF.1:P-Synch)

The TSF shall be capable of performing the following security management functions: *modification of the global password policy, management of user objects, modification of administrative user passwords.* FMT_SMF.1.1

5.1.4.5 Specification of Management Functions (FMT_SMF.1:ID-Synch)

The TSF shall be capable of performing the following security management functions: *modification of the global password policy, management of user objects and access control groups, modification of administrative user passwords.* FMT_SMF.1.1

5.1.4.6 Security roles (FMT_SMR.1:P-Synch)

The TSF shall maintain the roles *super user, help desk user, and regular user*. FMT_SMR.1.1

5.1.4.7 Security roles (FMT_SMR.1:P-Synch)

The TSF shall maintain the roles *super user, console user, and regular user*. FMT_SMR.1.1

Note: Collectively, super users, help desk users, and console users are referred to as “administrative users”.

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

5.1.5 Protection of the TOE security functions **(FPT)**

5.1.5.1 Basic internal TSF data transfer protection (FPT_ITT.1)

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

5.2 TOE security assurance requirements

The Evaluation Assurance Level chosen for this evaluation is 2 (EAL2). EAL2 was chosen to provide a low to moderate level of independently assured security based on availability of the complete development record from the vendor. The chosen assurance level is consistent with the postulated threat environment. EAL2 was chosen to provide: a low to moderate level of assurance that is consistent with good commercial practices.

The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain).

EAL2 also provides assurance through a configuration list for the TOE, and evidence of secure delivery procedures.

The TOE's permutational and combinatory mechanisms (passwords) will provide strength of function consistent with corporate password requirements in terms character length and numeric / alphabetic content in accordance with FIA_SOS.1 above.

Table 5-3 Assurance Requirements for EAL2

Assurance Class	Assurance Components
ACM	ACM_CAP.2
ADO	ADO_DEL.1 ADO_IGS.1
ADV	ADV_FSP.1 ADV_HLD.1 ADV_RCR.1
AGD	AGD_ADM.1 AGD_USR.1
ATE	ATE_COV.1 ATE_FUN.1 ATE_IND.2
AVA	AVA_SOF.1 AVA_VLA.1

5.2.1 Configuration management (ACM)

5.2.1.1 Configuration items (ACM_CAP.2)

The developer shall provide a reference for the TOE.$^{\text{ACM\_CAP.2.1D}}$

The developer shall use a CM system.$^{\text{ACM\_CAP.2.2D}}$

The developer shall provide CM documentation.$^{\text{ACM\_CAP.2.3D}}$

The reference for the TOE shall be unique to each version of the TOE.$^{\text{ACM\_CAP.2.1C}}$

The TOE shall be labelled with its reference.$^{\text{ACM\_CAP.2.2C}}$

The CM documentation shall include a configuration list.$^{\text{ACM\_CAP.2.3C}}$

The configuration list shall describe the configuration items that comprise the TOE.$^{\text{ACM\_CAP.2.4C}}$

The CM documentation shall describe the method used to uniquely identify the configuration items.$^{\text{ACM\_CAP.2.5C}}$

The CM system shall uniquely identify all configuration items that comprise the TOE.$^{\text{ACM\_CAP.2.6C}}$

5.2.2 Delivery and operation **(ADO)**

5.2.2.1 Delivery procedures (ADO_DEL.1)

The developer shall document procedures for delivery of the TOE or parts of it to the user. $^{\text{ADO\_DEL.1.1D}}$

The developer shall use the delivery procedures. $^{\text{ADO\_DEL.1.2D}}$

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.$^{\text{ADO\_DEL.1.1C}}$

5.2.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE. $^{\text{ADO\_IGS.1.1D}}$

The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE. $^{\text{ADO\_IGS.1.1C}}$

5.2.3 Development **(ADV)**

5.2.3.1 Informal functional specification (ADV_FSP.1)

The developer shall provide a functional specification.$^{\text{ADV\_FSP.1.1D}}$

The functional specification shall describe the TSF and its external interfaces using an informal style.$^{\text{ADV\_FSP.1.1C}}$

The functional specification shall be internally consistent.$^{\text{ADV\_FSP.1.2C}}$

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions, and error messages, as appropriate.$^{\text{ADV\_FSP.1.3C}}$

The functional specification shall completely represent the TSF.$^{\text{ADV\_FSP.1.4C}}$

5.2.3.2 Descriptive high-level design (ADV_HLD.1)

The developer shall provide the high-level design of the TSF.$^{\text{ADV\_HLD.1.1D}}$

The presentation of the high-level design shall be informal.$^{\text{ADV\_HLD.1.1C}}$

The high-level design shall be internally consistent.$^{\text{ADV\_HLD.1.2C}}$

The high-level design shall describe the structure of the TSF in terms of subsystems.$^{\text{ADV\_HLD.1.3C}}$

The high-level design shall describe the security functionality provided by each subsystem of the TSF.$^{\text{ADV\_HLD.1.4C}}$

The high-level design shall identify any underlying hardware, firmware, and / or software required by the

TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.$^{\text{ADV\_HLD.1.5C}}$

The high-level design shall identify all interfaces to the subsystems of the TSF.$^{\text{ADV\_HLD.1.6C}}$

The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.$^{\text{ADV\_HLD.1.7C}}$

5.2.3.3 Informal correspondence demonstration (ADV_RCR.1)

The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.$^{\text{ADV\_RCR.1.1D}}$

For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.$^{\text{ADV\_RCR.1.1C}}$

5.2.4 Guidance documents **(AGD)**

5.2.4.1 Administrator guidance (AGD_ADM.1)

The developer shall provide administrator guidance addressed to system administrative personnel.$^{\text{AGD\_ADM.1.1D}}$

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.$^{\text{AGD\_ADM.1.1C}}$

The administrator guidance shall describe how to administer the TOE in a secure manner.$^{\text{AGD\_ADM.1.2C}}$

The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.$^{\text{AGD\_ADM.1.3C}}$

The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.$^{\text{AGD\_ADM.1.4C}}$

The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.$^{\text{AGD\_ADM.1.5C}}$

The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.$^{\text{AGD\_ADM.1.6C}}$

The administrator guidance shall be consistent with all other documentation supplied for evaluation.$^{\text{AGD\_ADM.1.7C}}$

The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.$^{\text{AGD\_ADM.1.8C}}$

5.2.4.2 User guidance (AGD_USR.1)

The developer shall provide user guidance.[AGD_USR.1.1D]

The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE. [AGD_USR.1.1C]

The user guidance shall describe the use of user-accessible security functions provided by the TOE.[AGD_USR.1.2C]

The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.[AGD_USR.1.3C]

The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.[AGD_USR.1.4C]

The user guidance shall be consistent with all other documentation supplied for evaluation.[AGD_USR.1.5C]

The user guidance shall describe all security requirements for the IT environment that are relevant to the user.[AGD_USR.1.6C]

5.2.5 Tests **(ATE)**

5.2.5.1 Evidence of coverage (ATE_COV.1)

The developer shall provide evidence of the test coverage.[ATE_COV.1.1D]

The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.[ATE_COV.1.1C]

5.2.5.2 Functional testing (ATE_FUN.1)

The developer shall test the TSF and document the results.[ATE_FUN.1.1D]

The developer shall provide test documentation.[ATE_FUN.1.2D]

The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.[ATE_FUN.1.1C]

The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.[ATE_FUN.1.2C]

The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.[ATE_FUN.1.3C]

The expected test results shall show the anticipated outputs from a successful execution of the tests.[ATE_FUN.1.4C]

The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.[ATE_FUN.1.5C]

5.2.5.3 Independent testing - sample (ATE_IND.2)

The developer shall provide the TOE for testing.[ATE_IND.2.1D]

The TOE shall be suitable for testing.[ATE_IND.2.1C]

The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF. [ATE_IND.2.2C]

5.2.6 Vulnerability assessment (AVA)

5.2.6.1 Strength of TOE security function evaluation (AVA_SOF.1)

The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.[AVA_SOF.1.1D]

For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP / ST.[AVA_SOF.1.1C]

For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP / ST.[AVA_SOF.1.2C]

5.2.6.2 Developer vulnerability analysis (AVA_VLA.1)

The developer shall perform a vulnerability analysis. [AVA_VLA.1.1D]

The developer shall provide vulnerability analysis documentation. [AVA_VLA.1.2D]

The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP. [AVA_VLA.1.1C]

The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities. [AVA_VLA.1.2C]

The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE. [AVA_VLA.1.3C] [AVA_VLA.1.1C]

5.3 Security requirements for the IT environment

5.3.1 Protection of the TOE security functions (FPT)

5.3.1.1 Non-bypassability of the TSP (FPT_RVM.1)

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.$^{\text{FPT\_RVM.1.1}}$

5.3.1.2 TSF domain separation (FPT_SEP.1)

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.$^{\text{FPT\_SEP.1.1}}$

The TSF shall enforce separation between the security domains of subjects in the TSC.$^{\text{FPT\_SEP.1.2}}$

5.3.1.3 Reliable time stamps (FPT_STM.1)

The TSF shall be able to provide reliable time stamps for its own use. $^{\text{FPT\_STM.1.1}}$

5.3.1.4 User authentication before any action (FIA_UAU.2:Users) The TSF shall require each user *not assigned to an administrative user role* to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.$^{\text{FIA\_UAU.2.1:Users}}$

5.4 Statement of strength of TOE security function

Strength of function, as a CC concept, applies to probabilistic or permutational mechanisms that are non-cryptographic in nature. This ST claims AVA_SOF.1 applicability for the user identification and authentication SFR FIA_UAU.2 through the user password entry function and its mechanism.

The minimum strength of function level for the password entry mechanism through the application of FIA_SOS.1 above is calculated from the password rules elaborated in Section 6 on Page 31 of this ST.

The TOE claims SOF-high.

6 TOE Summary Specification

6.1 Statement of TOE IT security functions

ITSF.Audit The TOE implements audit functions by recording events listed in Table 5-2 Auditable Events on Page 16. The TOE associates the event record with the account name causing the event to be generated. The TOE also implements reporting facilities enabling the selective review of the data by administrative users.

ITSF.I&A The TOE implements the user Identification and Authorization services required to manage access requests of individual users in accordance with the *Protected User Record Access Control* policy.

When a user launches the web application he or she must provide a login ID and password. If the user is an administrative user, the TOE compares the supplied password to the user's hashed password stored in the identity cache. If the user is a regular user, the TOE uses a back-end authentication method to verify the supplied password against one of the user's accounts in the IT environment. If the comparison or verification is successful, and if the user status is not disabled or locked, the TOE grants the user access. If the number of consecutive unsuccessful authentication attempts exceeds the threshold (three by default) the offending user ID is locked until unlocked by an administrative user.

Strength of function claims apply to this IT security function based on the following password rules:

- have at least 6 character(s)
- have at least 3 letter(s)
- have at least 1 digit(s)
- not be your account name with the letters rearranged
- have no more than 2 pair(s) of repeating characters

ITSF.DAC The TOE implements a discretionary access control policy called *Protected User Record Access Control* defined as follows:

- Subjects are defined as the human user or a proxy acting on the user's behalf and identified by account name, user role, and password;
- Objects are defined as the global password policy, audit data, user objects, and access control groups held by the TOE;
- Operations managed by this access control policy are:
  - Modification of the global password policy is limited to administrative users with the appropriate right.
  - The viewing of audit data is limited to administrative users with the appropriate right.
  - The management of access control groups is limited to administrative users with the appropriate rights.
  - The management of administrative user objects is limited to administrative users with the appropriate right.
    Additionally, an administrative user can only manage administrative user objects that have equal or lesser rights. An administrative user cannot modify his own user rights.
  - The management of "manually added" regular user objects is limited to administrative users with the appropriate right.

Note the following:

- The *addition* of regular users is an automatic process, where ID Management Suite imports the account name from the IT environment (target systems).
- Account names and role type (administrative user or regular user) cannot be modified.
- Access control groups assign regular users (authorizers, requesters, and recipients) with read and write access to user profile data attributes in ID-Synch.

ITSF.Secure_Transfer The TOE implements validated data encryption in its protocol stack in order to protect the managed data while in transit from one part of the TOE to another.

6.2 Assurance measures

Table 6-1 Assurance Measures

Assurance Components	Description	Compliance
ACM_CAP.2	Evaluation of CM capabilities	TOE releases are identified with a unique version number. All Configuration Items that comprise the TOE are under Configuration Management and are included on a Configuration List. The CM system (described in the CM plan) shall provide measures such that only authorized changes are made to the configuration items.
ADO_DEL.1	Delivery procedures	The developer implements documented electronic delivery procedures using certified public-key mechanisms to prevent modification of the TOE in transit.
ADO_IGS.1	Installation, generation, and start-up	The TOE is supplied with detailed installation, generation and start-up procedures to ensure that the TOE is initialized in a manner that will reproducibly place it in a secure initial state.
ADV_FSP.1	Informal functional specification	The document “Functional Specification Document” provides a set of informal functional specifications describing the TSF and its external internal interfaces.
ADV_HLD.1	Evaluation of high level design	The document “High-Level Design Document” describes, in an informal manner, the TSF design, its subsystems and interfaces, and the security functionality provided by the subsystems.

. . . continued on the next page

Table 6-1 continued

Assurance Components	Description	Compliance
ADV_RCR.1	Informal correspondence demonstration	A representational correspondence is supplied correlating adjacent TOE representation pairs, namely: • ST TOE summary specifications to the informal functional specification, • the informal functional specification to the high-level design.
AGD_ADM.1	Administrator guidance	Administrator guidance is provided with the TOE to provide administrators with the required knowledge to securely configure and maintain the TOE within the environment.
AGD_USR.1	User guidance	User guidance is provided with the TOE to supply the (non-privileged) user with the required knowledge to operate in a secure manner and describes all security information relevant to the user.
ATE_COV.1	Evaluation of coverage	The analysis of test coverage provided demonstrates that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.
ATE_FUN.1	Functional testing	Functional testing of all security functions is performed to demonstrate that the functions perform as specified. Test documentation is provided detailing test plans, descriptions, expected and actual results.
ATE_IND.2	Independent testing - sample	The TOE and developer's test documentation will be available for independent testing.
AVA_SOF.1	Strength of TOE security function evaluation	The TOE Strength of Function Analysis quantifies the TOE's password mechanism strength and demonstrates it meets the requirements specified in FIA_SOS.1 above.

. . . continued on the next page

Table 6-1 continued

Assurance Components	Description	Compliance
AVA_VLA.1	Developer vulnerability analysis	The TOE vulnerability analysis is performed to ascertain the presence of obvious security vulnerabilities, and to confirm that they cannot be exploited in the intended environment for the TOE.

7 PP Claims

Hitachi ID's ID Management Suite does not claim conformance to any CC Protection Profile (PP).

8 Rationale

8.1 Introduction

The purpose of this section is to show that the security objectives of the TOE are appropriate to the security problem defined in the security environment section (see Section 3 on Page 12). This is accomplished through a set of tables that cross-reference threats, security policies, and assumptions against the security objectives that address them. Each threat, policy, or assumption is addressed by one or more security objective. Each security objective of the TOE (described in Section 4 on Page 14) addresses at least one threat, policy, or assumption. An informal argument is provided to show, for each threat, policy, or assumption, why the identified security objective provides an effective countermeasure that prevents an attack or mitigates risk to acceptable levels.

8.2 Security objectives rationale

Table 8-1 Mapping the TOE Security Environment to Security Objectives

Security Objectives and Assumptions Policy, Threats and Assumptions	O.Audit	O.I&A	O.Secure_Transfer	O.User_Defined _AC	OE.Audit	OE.AC	OE.Back_End_Auth	OE.Competent_Admin	OE.Coop_User	OE.Environment	OE.Network	OE.Physical	OE.Ext_Services	Rationale
T.Disclosure			X											By encrypting the data while it transits between remote parts of the TOE, it is possible to ensure that anyone attempting to capture the data will be unable to recover meaningful data.
P.Accountability	X	X		X										By implementing identification and authentication of individual users and enforcing discretionary access controls and auditing controls by the TOE, it is possible to prevent unauthenticated changes to the TOE data and to assign individual accountability for legitimate actions.

. . . continued on the next page

Table 8-1 continued

Security Objectives and Assumptions Policy, Threats and Assumptions	O.Audit	O.I&A	O.Secure_Transfer	O.User_Defined _AC	OE.Audit	OE.AC	OE.Back_End_Auth	OE.Competent_Admin	OE.Coop_User	OE.Environment	OE.Network	OE.Physical	OE.Ext_Services	Rationale
A.Time_Source					X									By implementing a reliable time source for time stamping audit records, the IT environment provides the date and time components of the audit records.
A.Reference_Monitor						X								By implementing a properly implemented reference monitor and enforcing domain separation, the TOE's environment allows the TOE to implement the access controls.
A.Back_End_Auth							X							By providing back-end authentication on non-administrative users, the IT environment ensures that users in non-administrative roles are properly authenticated.
A.Competent_Admin								X						By ensuring that system administrators are competent to manage the TOE and the security of the information it contains, the TOE's environment ensures that administrators will not compromise the security of the TOE or its data either willfully or by neglect.

. . . continued on the next page

Table 8-1 continued

Security Objectives and Assumptions Policy, Threats and Assumptions	O.Audit	O.I&A	O.Secure_Transfer	O.User_Defined _AC	OE.Audit	OE.AC	OE.Back_End_Auth	OE.Competent_Admin	OE.Coop_User	OE.Environment	OE.Network	OE.Physical	OE.Ext_Services	Rationale
A.Coop_User									X					By implementing procedures to maintain user cooperation, the TOE ensures that users will cooperate with those responsible for managing the TOE, to maintain TOE security and will follow all directives and prescriptions imposed by the administrators and / or guidance provided with the TOE.
A.Environment										X				By providing a secure environment for the TOE, the IT environment ensures that the TOE is secure and that the administrators have a good working knowledge and know how to manage the OS underlying the TOE.
A.Network											X			By implementing a secure network, the TOE's environment can ensure that the TOE is protected from active network attacks (i.e. data mode intrusion).
A.Physical												X		By implementing an environment providing physical security adequate to protect against unauthorized access, the TOE's environment can ensure that TOE is physically secure.

. . . continued on the next page

Table 8-1 continued

Security Objectives and Assumptions / Policy, Threats and Assumptions	O.Audit	O.I&A	O.Secure_Transfer	O.User_Defined _AC	OE.Audit	OE.AC	OE.Back_End_Auth	OE.Competent_Admin	OE.Coop_User	OE.Environment	OE.Network	OE.Physical	OE.Ext_Services	Rationale
A.Ext_Services													X	By providing secure external services, the IT environment ensures that the services do not offer unauthorized access to the TOE.

8.3 Security functional requirements rationale

Table 8-2 Mapping Security Objectives to Security Functional Requirements

Security Objectives and Assumptions / Policy, Threats and Assumptions	O.Audit	O.I&A	O.Secure_Transfer	O.User_Defined _AC	OE.Audit	OE.AC	OE.Back_End_Auth	Rationale
TOE Security Requirements								
FAU_ADG.1	X							The TOE maintains a session log (“SESSLOG”) in the database tracking the items listed in “Table 5-2 Auditable Events” on Page 16.
FAU_GEN.2	X							Auditable events generated by FAU_ADG.1 are associated with the account name responsible for the generation of the event.
FAU_SAR.1	X							Review of the audit trail records is done using the built-in reporting facility. Access to the reporting facility is limited to administrative users. Using the reporting facility, administrative users with the specified right can run reports on the entire audit database and generate human-readable reports.

. . . continued on the next page

Table 8-2 continued

Security Objectives and Assumptions Policy, Threats and Assumptions	O.Audit	O.I&A	O.Secure_Transfer	O.User_Defined _AC	OE.Audit	OE.AC	OE.Back_End_Auth	Rationale
FAU_SAR.2				X				Users must be granted explicit permission to use the reporting facility. Other users are prohibited from accessing the audit data and report facility.
FAU_SAR.3:P-Synch FAU_SAR.3:ID-Synch	X							The reporting facility accepts user-defined filters for the elaboration of audit trail reports. In P-Synch, users can search on account name, event type, and / or date; in ID-Synch, users can search on operation, target system, and / or date. The TOE also comes with pre-packaged reports.
FAU_STG.1				X				The TOE prevents modification of the audit records by restricting write access to the audit trail. All access to the audit trail is done through utilities included with the TOE and thus restricted to well-defined actions based on the user's privileges.
FDP_ACC.1				X				FDP _ACC.1 and FDP_ACF.1 implement a subset discretionary access control, which requires that the *Protected User Record Access Control* policy be enforced on subjects, objects and operations.
FDP_ACF.1:P-Synch FDP_ACF.1:ID-Synch				X				FDP_ACC.1 and FDP_ACF.1 implement a subset discretionary access control, which requires that the *Protected User Record Access Control* policy be enforced on subjects, objects and operations.
FIA_AFL.1		X						The TOE disables a user after the defined number of unsuccessful authentication attempts has been met. This is 3 by default. Users remain disabled until re-enabled (unlocked) by an administrative user.
FIA_ATD.1:P-Synch FIA_ATD.1:ID-Synch		X						For each user registered, the TOE maintains (at a minimum) the individual attributes: account name, user role, user rights, access control group (ID-Synch), and administrative user password.

. . . continued on the next page

Table 8-2 continued

Security Objectives and Assumptions Policy, Threats and Assumptions	O.Audit	O.I&A	O.Secure_Transfer	O.User_Defined _AC	OE.Audit	OE.AC	OE.Back_End_Auth	Rationale
FIA_SOS.1		X						The TOE's password mechanism is implemented so that an attack is curtailed–the offending user ID is locked out–after an administrator configurable number of consecutive, unsuccessful, authentication attempts. This is three by default. The offending user ID remains locked until unlocked by and administrative user. Thus, a strength rating of SOF-High is met based on the low probability of a correct guess in those few attempts, and the TOE's resistance to other vulnerabilities and types of attacks (such as social engineering attacks). The probability of guessing users' passwords is based on the default password policy rules described in Section 6 on Page 31. In addition, the TOE included a built-in password policy engine with over 50 standard rules plus a regular expression engine and plug-in system, allowing organizations to define new rules. Open-ended password history and dictionary checks are included.
FIA_UAU.2:Admin		X						Users are identified and authenticated prior to any transaction involving the data protected by the TOE. The TOE requires the user or the proxy acting on behalf of the user to identify the user; this is used to select the record to be accessed. Prior to supplying the credentials on behalf of the user of accepting a transaction on a user record, the user must also be authenticated.
FIA_UAU.7		X						During the authentication process, the user is provided with feedback which is obscured in a way that is consistent with the method of authentication, e.g. asterisks or blocks in web forms.

. . . continued on the next page

Table 8-2 continued

Security Objectives and Assumptions Policy, Threats and Assumptions	O.Audit	O.I&A	O.Secure_Transfer	O.User_Defined_AC	OE.Audit	OE.AC	OE.Back_End_Auth	Rationale
FIA_UID.2		X						Users are identified and authenticated prior to any transaction involving the data protected by the TOE. The TOE requires the user or the proxy acting on behalf of the user to identify the user; this is used to select the record to be accessed. Prior to supplying the credentials on behalf of the user of accepting a transaction on a user record, the user must also be authenticated.
FIA_USB.1:P-Synch FIA_USB.1:ID-Synch		X						The TOE forces any subject to select and authenticate to a valid account name. This account name is then used to enforce the *Protected User Record Access Control* policy and to associate auditable events to a user.
FMT_MSA.1:P-Synch				X				The TOE enforces the *P-Synch Protected User Record Access Control* policy DAC by limiting the ability to change the security attributes: password policy rules, audit data records, administrative user passwords, account name, user rights, and user profile data to authorized users.
FMT_MSA.1:ID-Synch				X				The TOE enforces the *ID-Synch Protected User Record Access Control* policy DAC by limiting the ability to change the security attributes: password policy rules, audit data records, administrative user passwords, account name, user rights, user profile data, and group members to authorized users.
FMT_MSA.3				X				The TOE initializes administrative users with no rights. Rights must be explicitly selected by the administrative user object's creator. The TOE initializes regular user objects with only the most basic rights.

. . . continued on the next page

Table 8-2 continued

Security Objectives and Assumptions Policy, Threats and Assumptions	O.Audit	O.I&A	O.Secure_Transfer	O.User_Defined_AC	OE.Audit	OE.AC	OE.Back_End_Auth	Rationale
FMT_SMF.1:P-Synch FMT_SMF.1:ID-Synch				X				The TOE enables authorized administrators to manage security attributes for the global password policy, access control groups (ID-Synch), user objects, and administrative user passwords. The TOE allows that privileges be assigned to administrative users to enable them to carry out management functions.
FMT_SMR.1:P-Synch FMT_SMR.1:ID-Synch				X				The TOE internally maintains for its own use the following roles: super user, help desk user (P-Synch), console user (ID-Synch), and regular user. User accounts are associated to one of these roles.
FPT_ITT.1			X					The TOE protects data from disclosure during transfers between separate parts of the TOE by implementing a certified implementation of AES-128 (AES certificate #236, CBC(e/d; 128)) in its network protocol stack and encrypting / decrypting protected data while in transit.
IT Environment Security Requirements								
FIA_UAU.2:Users							X	The IT environment must provide back-end authentication services to authenticate users not assigned to administrative roles.
FPT_RVM.1						X		The IT environment must enforce the non-bypassability of the TOE security policy by ensuring that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed

. . . continued on the next page

Table 8-2 continued

Security Objectives and Assumptions Policy, Threats and Assumptions	O.Audit	O.I&A	O.Secure_Transfer	O.User_Defined _AC	OE.Audit	OE.AC	OE.Back_End_Auth	Rationale
FPT_SEP.1						X		The IT environment must provide and maintain a security domain for the exclusive use of the TOE. It must prevent interference and tampering by untrusted subjects.
FPT_STM.1					X			The IT environment must provide a reliable time stamp for use in the auditing mechanism of the TOE.

Table 8-3 Mapping TOE IT Security Functions to Security Function Requirements

IT Security Functions	SFRs	Rationale
ITSF.DAC	FDP_ACC.1 FDP_ACF.1:P-Synch FDP_ACF.1:ID-Synch FMT_MSA.1:P-Synch FMT_MSA.1:ID-Synch FMT_MSA.3 FMT_SMF.1:P-Synch FMT_SMF.1:ID-Synch FMT_SMR.1:P-Synch FMT_SMR.1:ID-Synch FAU_SAR.2 FAU_STG.1	The TOE implements FDP_ACC.1 by enforcing the *Protected User Record Access Control,* the TOE's Discretionary Access Control Policy is enforced and allows authorized users to perform operations allowed under the policy. The TOE implements FDP_ACF.1:P-Synch and FDP_ACF.1:ID-Synch by enforcing that attributes are associated with subjects and objects, and by enforcing rules among controlled objects and subjects. Subjects include administrative users and regular users; objects include the global password policy, audit data, user objects, and access control groups (ID-Synch). This supports the enforcement of DAC policy expressed by FDP_ACF.1. The TOE implements FMT_MSA.1:P-Synch and FMT_MSA.1:ID-Synch by enforcing for the TSF's ability to restrict the modification of the security attributes of managed objects to authorized subjects in accordance with the *Protected User Record Access Control*. Specifically, administrative users with the appropriate rights may modify the global password policy, user objects, access control groups (ID-Synch), and administrative user passwords. The TOE implements FMT_MFA.3 by managing objects with restrictive default discretionary access control values based on the SFP. The TOE implements FMT_SMF.1:P-Synch and FMT_SMF.1:ID-Synch by allowing administrative users to modify the global password policy, manage user objects, manage access control groups (ID-Synch), and modify administrative user passwords. The TOE implements FMT_SMR.1:P-Synch and FMT_SMR.1:ID-Synch by allowing the TOE to identify various roles in order to assign role-based permissions consistent with the SFP.

. . . continued on the next page

Table 8-3 continued

IT Security Functions	SFRs	Rationale
		The TOE implements FAU_SAR.2 by restricting the read access to the audit records to users that have been granted explicit read-access. The TOE implements FAU_STG.1, by protecting the stored audit records from unauthorized deletion and prevents modifications to the audit records; guaranteeing the integrity of the audit records.
ITSF.Audit	FAU_ADG.1 FAU_GEN.2 FAU_SAR.1 FAU_SAR.3:P-Synch FAU_SAR.3:ID-Synch	The TOE implements FAU_ADG.1 and FAU_GEN.2 by providing for the generation of audit records for selected events and the ability for the TSF to associate each auditable event with the identity of the user that caused the event. The TOE implements FAU_SAR.1 providing administrative users with the capability to read all audit information from the audit records. The TOE's reporting facility ensures that the audit records are presented in a manner suitable for the user to interpret the information. The TOE implements FAU_SAR.3 by enabling the ability to perform searches of specified types on the audit records.
ITSF.Secure_Transfer	FPT_ITT.1	The TOE implements FPT_ITT.1 to protect the TSF data from disclosure when transmitted between separate parts of the TOE by the inclusion of a certified implementation of AES-128 (AES certificate #236, CBC(e/d; 128)) in the TSF's network protocol stack and encrypting / decrypting protected data while in transit.

. . . continued on the next page

Table 8-3 continued

IT Security Functions	SFRs	Rationale
ITSF.I&A	FIA_AFL.1 FIA_ATD.1:P-Synch FIA_ATD.1:ID-Synch FIA_SOS.1 FIA_UAU.2 FIA_UID.2 FIA_UAU.7 FIA_USB.1:P-Synch FIA_USB.1:ID-Synch	The TOE implements FIA_AFL to detect when the threshold for unsuccessful authentication attempts has been exceeded by a user and to disable the user. The TOE implements FIA_ATD.1 to provide that the TSF maintain the account name, user role, user rights, access control groups (ID-Synch), and administrative user passwords that enable identification and authentication of users. The TOE implements FIA_SOS.1 by enforcing default password rules mentioned in Section 6 on Page 31. The TOE implements FIA_UAU.2 and FIA_UID.2 to force the user to submit their credentials for identification and authentication prior to allowing any operation to be performed. These requirements collectively ensure that only authorized users gain access to the TOE and its resources and maintain accountability for user actions by enabling the TSF to associate actions with account names. The TOE implements FIA_UAU.7 to prevent the disclosure of user password information during login. The TOE implements FIA_USB.1 to associate the above user security attributes with subjects acting on the behalf of that user.

8.4 Assurance security requirements rationale

This TOE is intended to be deployed in an environment presenting a low level of threats from attackers presenting low levels of knowledge and motivation. As a result, the developers require a low to moderate level of independently assured security. EAL2 was selected because the co-operation of the developer was available in terms of the delivery of design information and test results.

8.5 Dependencies rationale

This section will demonstrate that all dependencies have been satisfied and that no unsatisfied dependencies are left.

Table 8-4 Functional and Assurance Requirements Dependencies

Requirement	Dependencies
Functional Requirements	
FAU_ADG.1	FPT_STM.1[1]
FAU_GEN.2	FAU_GEN.1, FIA_UID.1
FAU_SAR.1	FAU_GEN.1 (satisfied by FAU_ADG.1, refer to rational above)
FAU_SAR.2	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1
FAU_STG.1	FAU_GEN.1 (satisfied by FAU_ADG.1, refer to rational above)
FDP_ACC.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3
FIA_AFL.1	FIA_UAU.1 (satisfied by FIA_UAU.2 which is hierarchical to FIA_UAU.1)
FIA_UAU.2	FIA_UID.1 (satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1)
FIA_UAU.7	FIA_UAU.1 (satisfied by FIA_UAU.2 which is hierarchical to FIA_UAU.1)
FIA_USB.1	FIA_ATD.1
FMT_MSA.1	FDP_ACC.1, FMT_SMF.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1:ID-Synch, FMT_SMR.1
FMT_SMR.1	FIA_UID.1 (satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1)
Assurance Requirements	
ADO_IGS.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1
ADV_HLD.1	ADV_FSP.1, ADV_RCR.1
AGD_ADM.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1

. . . continued on the next page

[1] Extended requirement based on the CC part 2 functional requirement FAU_GEN.1 which has a dependency on FPT_STM.1. We therefore include this dependency as well.

Table 8-4 continued

Requirement	Dependencies
ATE_COV.1	ADV_FSP.1, ATE_FUN.1
ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
AVA_SOF.1	ADV_FSP.1, ADV_HLD.1
AVA_VLA.1	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1