SECURITY TARGET

FOR

BIOSCRYPT™ INC. BIOSCRYPT™ ENTERPRISE FOR NT LOGON

VERSION 2.1.3

EWA Document No. 1360-013-350
Version 3.2, 8 June 2001

Prepared for:

Certification Body
Communications Security Establishment
P.O. Box 9703
Terminal
Ottawa, Ontario
K1G 3Z4

Prepared by:

Electronic Warfare Associates-Canada, Ltd.
275 Slater St., Suite 1600
Ottawa, Ontario
K1P 5H9

SECURITY TARGET

FOR

BIOSCRYPT™ INC. BIOSCRYPT™ ENTERPRISE FOR NT LOGON

VERSION 2.1.3

Document No. 1360-013-350
Version 3.2, 8 June 2001

<Original> Approved by:

ST Author:	F. Wallace Peers	
Program Director:		
	(Signature)	(Date)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 IDENTIFICATION

This document details the Security Target (ST) for the Bioscrypt™ Enterprise version 2.1.3 biometric authentication package. The package includes both software and a serial biometric scanner. This ST has been prepared in accordance with the Common Criteria for Information Technology Security Evaluation (CC), version 2.1, August 1999.

1.2 OVERVIEW

Bioscrypt™ Enterprise is a fingerprint based, biometric based authentication package comprised of a hardware Bioscrypt™ Enterprise Reader and software libraries for Windows NT systems. The package replaces the normal Windows graphical identification and authentication (GINA) library. This allows a user's password to be replaced with a fingerprint through an enrolment process. Users authenticate by entering their username and then place their finger on the Bioscrypt™ Enterprise Reader (BER). Bioscrypt™ Enterprise compares the user's finger to the user's stored template, and if they match, opens a user session to the operating system (OS). A typical Bioscrypt™ Enterprise set-up for a Microsoft Windows domain is shown in Figure 1.

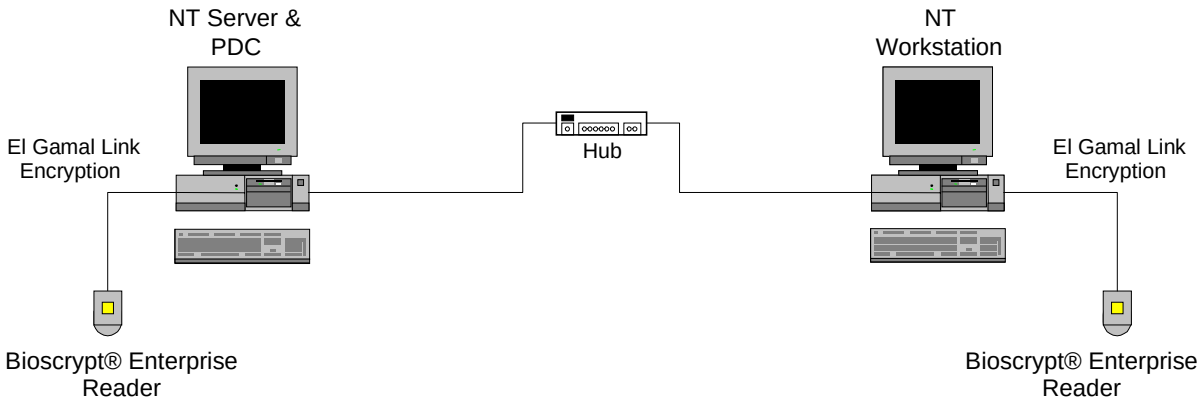

Figure 1: Example Bioscrypt™ Enterprise Installation for a Windows Domain

The main components of Bioscrypt™ Enterprise are the Bioscrypt™ Enterprise Reader, biometric reader control software (BRC), the replacement GINA, and the Bioscrypt™ database service. The Bioscrypt™ Enterprise Reader is connected to the host PC by a serial cable and communicates with the BRC. Communications between the PC and the scanner are protected by El Gamal encryption. The GINA makes calls to the BRC for user enrolment and authentication.

When a user's fingerprint is enrolled, Bioscrypt™ Enterprise manipulates the fingerprint to produce a Bioscrypt™ Template which is encrypted for confidentiality using Triple DES. The user's NT password is encrypted with a randomly generated user key using either DES or Triple DES depending on whether the product is the export or domestic version respectively. The pseudorandom number generator used to generate the user key depends on the version of the product: FIPS 186 in the export version, and ANSI X9.17 in the domestic. The user key is encrypted for confidentiality using Triple DES. The encrypted Bioscrypt™ Template, user key, and user password are appended together to create a Bioscrypt™ Collection (see Figure 3). The Bioscrypt™ Collection is then passed locally (in the case of a single workstation), or across the network (in the case of a NT domain) to the Bioscrypt™ Database Service which stores the Collection where the OS normally stores the user's password (ex. Windows SAM database). If the user is already enrolled, the Bioscrypt™ Collection is retrieved by the Bioscrypt™ Database Service and sent to the Bioscrypt™ Enterprise Reader for comparison with the user's fingerprint.

1.3 CC CONFORMANCE

The Target of Evaluation (TOE) for this ST is conformant with the functional requirements specified in Part 2 of the CC, and the assurance requirements for Evaluation Assurance Level (EAL) 2, as specified in Part 3 of the CC with the exception of the explicitly stated IT security functional requirements of FAU_ADG.1 and FPT_STP.1.

2 TARGET OF EVALUATION DESCRIPTION

Target of evaluation is the Bioscrypt™ Inc. Bioscrypt™ Enterprise biometric authentication package version 2.1.3 for Windows NT systems, as shown in Figure 2. The main components of the TOE are the Bioscrypt™ Enterprise Reader, BRC, the replacement GINA, and the Bioscrypt™ database service. There are two types of Bioscrypt™ Enterprise version 2.1.3, one for export, and one for domestic (United States and Canada); both are evaluated as a part of this ST. The only difference between the two types is the cryptographic algorithm used to encrypt the user's NT password (the export version uses DES and the domestic version uses Triple DES).

The DES and Triple DES algorithms have been evaluated and approved by a FIPS140-1 certified laboratory. El Gamal has not been formally tested as a part of this evaluation. The FIPS186 and ANSI X9.17 pseudorandom numbers generators have not been formally tested as a part of this evaluation.

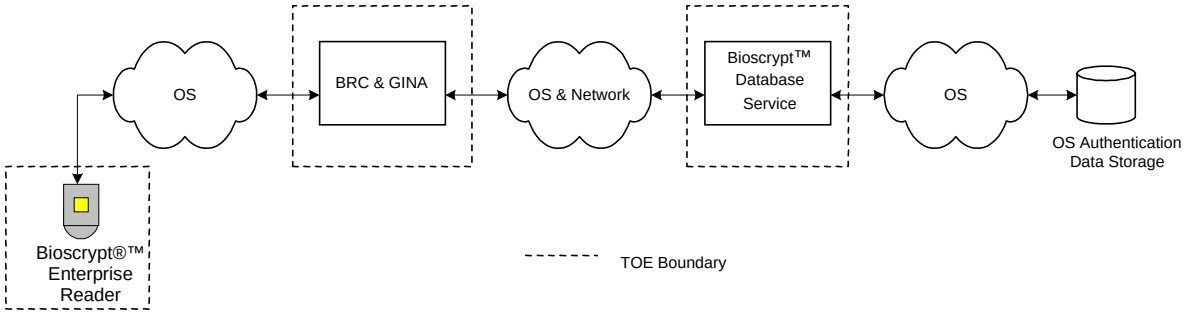

Figure 2: TOE Boundary Diagram

The Bioscrypt™ Enterprise Reader is a hardware device about the size of a mouse which connects to a host PC via a serial link. The centre of the reader contains a sensor. Users place their finger over the sensor and their fingerprint is digitally scanned. The BER contains a hard coded cryptographic key which is set during manufacturing by Bioscrypt™ Inc.. The hard coded key can be specified by the customer if desired. The BRC software is comprised of the software libraries which control the Bioscrypt™ Enterprise Reader. The Bioscrypt™ Enterprise GINA is a replacement for the normal Microsoft GINA. GINA controls the authentication sequence to the underlying OS and directs the biometric authentication process. The GINA will also allow normal username and password authentication by default, but a registry setting will force biometric authentication only. The evaluated TOE configuration requires this registry setting on all user's PCs with the exception of any PCs required for enrolment (see section 2.1:The Enrolment Process), and the Primary Domain Controller (only administrators should have access to the PDC).

Bioscrypt™ Enterprise can be installed on a stand alone workstation, or as part of a Windows Domain. In the case of a stand alone workstation, all components would be located on the

one PC, however for a domain, the Bioscrypt™ Database service must also be installed on the PDC in order for users to login across the network.

2.1 THE ENROLMENT PROCESS

Note: In order to enrol a user, the GINA on the enrol system must be configured to allow a user to authenticate via password and biometric fingerprint. The administrator must be present to verify the integrity of the enrolment system and the enrolment process for the user.

A user must have a pre-existing username and password in order to enrol. The user then attempts to login using a fingerprint. The GINA detects that the user does not have an existing Bioscrypt™ Collection, and prompts the user to enter their password. If the user correctly enters their password, the GINA gives the user the option to enrol. The GINA (through the BRC) prompts the user to scan their fingerprint three times; each scanned fingerprint image is displayed on the user's screen. The three images undergo a series of quality checks to ensure a good representation of the fingerprint has been captured, and are compared with each other to ensure consistency. If one or more of the images fails any of the checks, the user is asked to scan their fingerprint again. This process continues until three good images have been obtained or the user cancels the process.

The BRC then creates a Bioscrypt™ template from the images, which is used for comparison during the user's next login. The user password is encrypted at the BRC for confidentiality, either using DES (export version) or Triple DES (domestic version), with a randomly generated user key. The user key is appended to the Bioscrypt™ template then both are sent to the BER where they are encrypted with the hard coded key contained within the Bioscrypt™ Enterprise Reader (using Triple DES for confidentiality). The Bioscrypt™ is returned to the BRC where the encrypted password is appended to it. The encrypted template and user key, and password are called the Bioscrypt™ Collection, as shown in Figure 3. The collection is then transferred, using the normal OS channels for passwords, to the Bioscrypt™ Database Service. The Bioscrypt™ Database Service stores the Bioscrypt™ Collection in the same place that the OS normally stores the user passwords (ex. NT SAM database) using the OS channels for password storage.

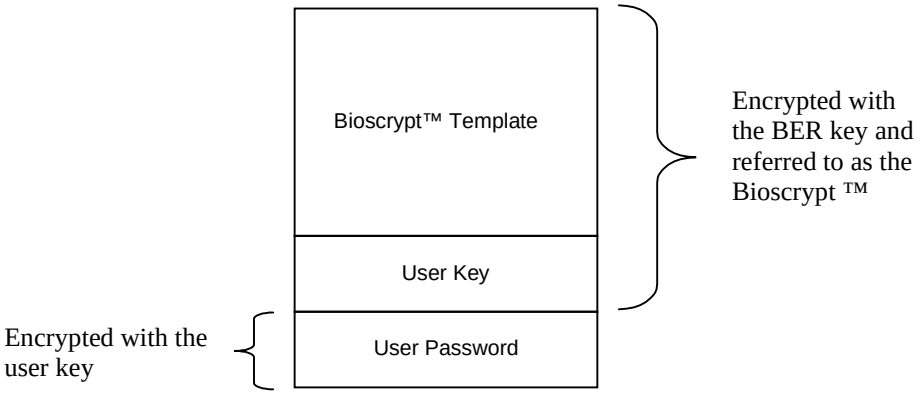

Figure 3: A Bioscrypt™ Collection

Users may only enrol one finger at a time. To re-enrol another finger, an OS administrator must remove the old Bioscrypt™ Collection from the OS authentication database using a utility included with Bioscrypt™ Enterprise. The user then enrols the new finger as stated previously.

2.2 THE VERIFICATION PROCESS

When the user initiates the OS login process, the GINA prompts the user to enter their username and scan their fingerprint. The GINA obtains the user's Bioscrypt™ from the Bioscrypt™ Database Service, and sends it to the Bioscrypt™ Enterprise Reader. The collection is unencrypted in the scanner and a current sample of the user's finger is compared to the stored template from the collection. If the finger and template match, the user key is sent to the BRC. The user password is unencrypted at the BRC, and sent (as if entered by the user) to the normal OS password authentication mechanisms. The user is thereby authenticated and a user session is opened. If the finger does not match the template, the authentication process is terminated and the user must start the process over again.

3 TOE SECURITY ENVIRONMENT

3.1 ASSUMPTIONS

The following conditions are assumed to exist in the operational environment:

A.NOEVIL Administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

A.TAMPER Authorised users are trusted not to tamper with the hardware (PC and biometric device).

A.PHYSEC Unauthorised users are not allowed unattended physical access to the hardware (workstations, servers, PDCs, BDCs, and biometric device).

A.CHECK During enrolment the administrator will verify that the serial link has not been tampered with.

3.2 THREATS

The following threats are addressed either by the TOE or the environment.

3.2.1 Threats Addressed By The TOE

The threats discussed below are addressed by a compliant TOE. The threat agents are either human users or external IT entities not authorised to use the TOE. The assets that are subject to attack are the IT resources protected by the TOE.

T.SNIFF A user may read a valid user's identification and authentication data as it is being transmitted between portions of the TOE or from where it is stored.

T.REPLAY An unauthorised user may capture valid user identification and authentication data, and use the identification and authentication data at a later time.

T.FAKE A user may present a fake physiological sample or otherwise create an imitation of valid biometric data which is accepted as legitimate by the TOE.

T.BIOTEMP A user may obtain access to residual biometric data which was not cleared after use.

T.FVRFY An individual may use their personal biometric data and be falsely verified as another valid user.

T.TOEATK A user may bypass, deactivate, or tamper with TOE hardware, firmware or software.

T.MODID An unauthorised user may create, modify, or delete the identification and authentication data stored in the TOE.

T.SHELL An individual may gain unauthorised access to another user's session after the user has been authenticated (e.g. after a valid user login).

T.UNDET An individual's attempts to falsely authenticate as a valid user may go undetected.

T.PASS An individual may obtain a valid user's password and use the password to authenticate as the valid user.

T.USAGE The TOE may be configured, used and administered in an insecure manner.

3.2.2 Threats To Be Addressed By Operating Environment

The threat possibilities discussed below must be countered by procedural measures and/or administrative methods:

T.TROJAN Compromise of the integrity and/or availability of the TOE may occur as a result of a TOE user unwittingly introducing a virus or trojan into the system.

T.ENROL An unauthorised user may enrol themselves as a valid user.

4 SECURITY OBJECTIVES

4.1 TOE SECURITY OBJECTIVES

The following are the IT security objectives for the TOE:

O.FALPOS The TOE must prevent faked or incorrect biometric data from being accepted as legitimate by the biometric device.

O.CRYPTO The TOE must protect the confidentiality of the biometric data using encryption.

O.ACL The TOE must enforce access control such that only authorised users may create, modify and delete security attributes. Only biometric authentication will be allowed (excluding the enrolment process where password authentication is required).

O.USER The TOE must provide functionality that enables users to effectively manage the TOE and its security functions from its human-machine interface (HMI).

O.AUDIT The TOE must generate a readable audit trail of security relevant events.

O.CLEAR The TOE must ensure no residual or unprotected biometric data remains after operations are completed.

O.LOCK The TOE must protect a user session against unauthorised access.

O.EXCH The TOE must exchange data between components of the TOE in a trusted manner.

4.2 ENVIRONMENT SECURITY OBJECTIVES

The following are non-IT security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

O.GUIDAN The users of the TOE must ensure that the TOE is delivered, installed, configured, administered, and operated in a manner that maintains its security.

O.VERIFY A method will exist such that all users' claimed identities will be reliably confirmed before enrolment.

O.TAMPER Authorised users do not tamper with the hardware (PC and biometric devices).

O.PHYPRO Controls and procedures must exist to prevent people from physically tampering with the TOE.

5 IT SECURITY REQUIREMENTS

5.1 TOE SECURITY REQUIREMENTS

This section provides functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance components from Part 3 of the CC, as well as the extended requirements: FAU_ADG.1 and FPT_STP.1.

5.1.1 Extended Security Functional Requirements:

FAU_ADG.1 Audit data generation

Hierarchical to: No other components

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

a. All auditable events for the [selection: *minimum, basic, detailed, not specified*] level of audit; and
b. [assignment: *other specifically defined auditable events*]

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

a. Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b. For each audit event type, based on the auditable event definitions of the functional components included in the ST, [assignment: *other audit relevant information*].

Dependencies: FPT_STM.1 Reliable time stamps

FPT_STP.1 SUBSET INTERNAL TSF DATA TRANSFER PROTECTION

Hierarchical to: No other components

FPT_STP.1.1 – The TSF shall protect TSF data from [selection: *disclosure, modification*] when it is transmitted between [assignment: *parts of the TOE*].

Dependencies: No Dependencies

5.1.2 TOE Security Functional Requirements

The functional security requirements for this ST are summarised in Table 1.

Application Note: A person's biometric characteristics are a direct representation of the user and can be arguably considered user data, however, for this ST the biometric characteristics are used to provided authentication and are therefore considered TSF data for the purposes of this evaluation.

Table 1 Summary of Security Functional Requirements

Functional Components	
Identifier	**Name**
FAU_ADG.1	Audit data generation
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FDP_ACC.2	Complete access control
FDP_ACF.1	Security attribute access control
FDP_RIP.1	Subset residual information protection
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.2	Generation of secrets
FIA_UAU.2	User authentication before any action
FIA_UAU.3	Unforgeable authentication
FIA_UAU.5	Multiple authentication mechanisms
FIA_UID.2	User identification before any action
FIA_USB.1	User-subject binding
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MTD.1	Management of TSF data
FPT_ITC.1	Inter-TSF confidentiality during transmission
FPT_STP.1	Subset internal TSF data transfer protection
FTA_SSL.1	TSF-initiated session locking
FTA_SSL.2	User-initiated locking
FTA_SSL.3	TSF-initiated termination

FAU_ADG.1 Audit data generation

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

a. All auditable events for the [not specified] level of audit; and
b. [unsuccessful logins.]

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

a. Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b. For each audit event type, based on the auditable event definitions of the functional components included in the ST, [none].

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 – The TSF shall generate cryptographic keys for the user in accordance with a specified cryptographic key generation algorithm [DES] and specified cryptographic key sizes [of 56 bits] that meet the following: [FIPS 186 standard] when using the export version of Bioscrypt™ Enterprise.

FCS_CKM.1.1 – The TSF shall generate cryptographic keys for the user in accordance with a specified cryptographic key generation algorithm [two key Triple DES in CBC mode] and specified cryptographic key sizes [112 bits] that meet the following: [ANSI X9.17 standard] when using the domestic version of Bioscrypt™ Enterprise.

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 – The TSF shall destroy the key used to encrypt the user's password (user key) cryptographic keys in accordance with a specified cryptographic key destruction method [by overwriting the old key with a new key; or by being encrypted by the Bioscrypt™ Enterprise reader's key and then deleted (this occurs if a user's Bioscrypt™ Collection is deleted)] that meets the following: [does not claim to meet an assigned standard].

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 – The TSF shall perform [encryption and decryption of the user's password] in accordance with a specified cryptographic algorithm [DES] and cryptographic key sizes [56 bits] that meet the following: [FIPS 46-3] when using the export version of Bioscrypt™ Enterprise.

FCS_COP.1.1 – The TSF shall perform [encryption and decryption of the user's password] in accordance with a specified cryptographic algorithm [two key Triple DES in CBC mode] and cryptographic key sizes [112 bits] that meet the following: [FIPS 46-3] when using the domestic version of Bioscrypt™ Enterprise.

FCS_COP.1.1 – The TSF shall perform [encryption and decryption of the user's Bioscrypt™ Template and the user's cryptographic key] in accordance with a specified cryptographic algorithm [two key Triple DES in CBC mode] and cryptographic key sizes [112 bits] that meet the following: [FIPS 46-3].

FDP_ACC.2 Complete access control

FDP_ACC.2.1 – The TSF shall enforce the [BIOMETRIC SFP[1]] on [

a. the NT login process acting on behalf of a user to enrol a biometric fingerprint;
b. the NT login process authenticating the user using fingerprint biometrics to access a graphical shell; and
c. the NT login process authenticating an administrator to remove a user's Bioscrypt™ Collection from the OS.]

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2 – The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 – The TSF shall enforce the [BIOMETRIC SFP[1]] on objects based on [username, the user's NT password, and the user's fingerprint].

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

a. [if the NT login process acting on behalf of the user has successfully authenticated with a username and password, enrol the user's fingerprint;

[1] The BIOMETRIC SFP defines the access control policy for the Bioscrypt® Enterprise. The policy is defined in FDP_ACF.1.2.

b. if the NT login process acting on behalf of a user provides a user's fingerprint that matches the enrolled fingerprint, then access is granted to the graphical shell; and
c. if the NT login process acting on behalf of an administrator has successfully authenticated and been granted access to the graphical shell, allow the administrator to delete a user's Bioscrypt™ Collection]

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

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

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 – The TSF shall ensure that any previous information content of memory is made unavailable upon the [de-allocation of memory from] the following objects: [Bioscrypt™ Enterprise Reader].

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 – The TSF shall detect when [an OS administrator defined number of] unsuccessful authentication attempts occur related to [biometric fingerprint authentication].

FIA_AFL.1.2 – When the defined number of unsuccessful biometric authentication attempts has been met or surpassed, the TSF shall [terminate the authentication process and/or lockout the user account as specified by the OS administrator].

FIA_ATD.1 User attribute definition

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

a. [username;
b. password; and
c. Bioscrypt™ Collection.]

FIA_SOS.2 Generation of secrets

FIA_SOS.2.1 – The TSF shall provide a mechanism to generate secrets that meet [a minimum level of distinct characteristics from the image of the user's fingerprint].

FIA_SOS.2.2 – The TSF shall be able to enforce the use of TSF generated secrets for [a fingerprint biometric authentication system].

FIA_UAU.2 User authentication before any action.

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

FIA_UAU.3 Unforgeable authentication

FIA_UAU.3.1 –The TSF shall [prevent] use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2 – The TSF shall [prevent] use of authentication data that has been copied from any other user of the TSF.

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 – The TSF shall provide [password and biometric fingerprint based authentication mechanisms] to support user authentication.

FIA_UAU.5.2 – The TSF shall authenticate any user's claimed identity according to the

a. using a password for enrolment only; and
b. using a biometric fingerprint for verification (enforced by a GINA registry setting)

FIA_UID.2 User identification before any action

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_USB.1 User-subject binding

FIA_USB.1 – The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 – The TSF shall enforce the [BIOMETRIC SFP] to restrict the ability to [add] the security attributes [Bioscrypt™ Collection] to [a user with a valid username and password].

FMT_MSA.1.1 – The TSF shall enforce the [BIOMETRIC SFP] to restrict the ability to [delete] the security attributes [Bioscrypt™ Collection] to [an OS administrator].

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 – The TSF shall ensure that only secure values are accepted for security attributes.

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 – The TSF shall restrict the ability to [modify, delete] the [GINA registry setting which forces the use of biometric authentication only (i.e. no password authentication allowed)] to [an OS administrator].

FPT_ITC.1 Inter-TSF confidentiality during transmission

FPT_ITC.1.1 – The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorised disclosure during transmission.

Application Note: The trusted product is the NT operating system. The Bioscrypt™ Collection is transmitted from the Bioscrypt™ Database Service and stored in the NT SAM file either locally for a stand-alone server or workstation, or remotely on the PDC for domains.

FPT_STP.1 Subset internal TSF data transfer protection

FPT_STP.1.1 – The TSF shall protect TSF data from [disclosure] when it is transmitted between [the BRC and the Bioscrypt™ Database Service].

FTA_SSL.1 TSF-initiated session locking

FTA_SSL.1.1 -- The TSF-shall lock an interactive session after [an administrator specified time period between 1 and 65535 seconds where no interactions between the user and the TOE occur] by:

a. clearing or overwriting display devices, making the current contents unreadable;
b. disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2 – The TSF shall require the following events to occur prior to unlocking the session: [user must re-authenticate].

FTA_SSL.2 User-Initiated locking

FTA_SSL.2.1 -- The TSF shall allow user-initiated locking of the user's own interactive session by:

a. clearing or overwriting display devices, making the current contents unreadable;
b. disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.2.2 – The TSF shall require the following events to occur prior to unlocking the session: [user must re-authenticate].

FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 – The TSF shall terminate a locked interactive session after an [administrator specified time period between 0 and 65535 seconds, where no interactions between the user and the TOE occur].

5.1.3 TOE Security Assurance Requirements

The security assurance requirements for EAL2, as specified in Part 3 of the CC, are summarised in Table 2.

Table 2 Assurance Requirements for Bioscrypt™ Enterprise

Assurance Class	Assurance Components	
	Identifier	**Name**
Configuration Management	ACM_CAP.2	Configuration Items
Delivery and Operation	ADO_DEL.1	Delivery Procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent testing – sample
Vulnerability Assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

ACM_CAP.2 Configuration items

Developer action elements:

ACM_CAP.2.1D – The developer shall provide a reference for the TOE.

ACM_CAP.2.2D – The developer shall use a configuration management (CM) system.

ACM_CAP.2.3D – The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.2.1C – The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C – The TOE shall be labelled with its reference.

ACM_CAP.2.3C – The CM documentation shall include a configuration list.

ACM_CAP.2.4C – The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.5C – The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.6C – The CM system shall uniquely identify all configuration items.

Evaluator action elements:

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

ADO_DEL.1 Delivery Procedures

Developer action elements:

ADO_DEL.1.1D – The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D – The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL1.1C – The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

ADO_DEL1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1 Installation, generation, and start-up procedures

Developer action elements:

ADO_IGS.1.1D – The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C – The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E – The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

ADV_FSP.1 Informal functional specification

Developer action elements:

ADV_FSP.1.1D – The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C – The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C – The functional specification shall be internally consistent.

ADV_FSP.1.3C – 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.

ADV_FSP.1.4C – The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E – The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

ADV_HLD.1 Descriptive high-level design

Developer action elements:

ADV_HLD.1.1D – The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C – The presentation of the high-level design shall be informal.

ADV_HLD.1.2C – The high-level design shall be internally consistent.

ADV_HLD.1.3C – The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C – The high-level design shall describe the security functionality provided by each subsystem of the TSF

ADV_HLD.1.5C – 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.

ADV_HLD.1.6C – The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C – The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

ADV_HLD.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E – The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_RCR.1.1D – The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representation that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C – 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.

Evaluator action elements:

ADV_RCR.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_ADM.1 Administrator guidance

Developer action elements:

AGD_ADM.1.1D – The developer shall provide administrator guidance addressed to system administration personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C – The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C – The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C – The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C – The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C – The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C – 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.

AGD_ADM.1.7C – The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C – The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_USR.1 User guidance

Developer action elements:

AGD_USR.1.1D – The developer shall provide user guidance.

Content and presentation of evidence elements:

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

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

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

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

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

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

Evaluator action elements:

AGD_USR.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_COV.1 Evidence of coverage

Developer action elements:

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

Content and presentation of evidence elements:

ATE_COV.1.1C – 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.

Evaluator action elements:

ATE_COV.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional testing

Developer action elements:

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

ATE_FUN.1.2D – The developer shall provide test documentation.

Content and presentation of evidence elements:

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

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

ATE_FUN.1.3C – 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.1.4C – The expected test results shall show the anticipated outputs from a successful execution of the tests.

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

Evaluator action elements:

ATE_FUN.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independent testing – sample

Developer action elements:

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

Content and presentation of evidence elements:

ATE_IND.2.1C – The TOE shall be suitable for testing.

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

Evaluator action elements:

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

ATE_IND.2.2E – The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E – The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

AVA_SOF.1 Strength of TOE security function evaluation

A typical attacker in the intended environment for the Bioscrypt™ Enterprise product is deemed to possess only limited knowledge biometric systems and lack the skills and resources required to manipulate the Bioscrypt™ Enterprise

reader. Therefore, for an EAL2 level evaluation of Bioscrypt™ Enterprise, the strength of function to meet or exceed for AVA_SOF calculations is BASIC. The Bioscrypt™ Enterprise system, configured at this security level, has a FAR of less than 0.001 (1/1000) at a 95% confidence level.

Developer action elements:

AVA_SOF.1.1D – 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.

Content and presentation of evidence elements:

AVA_SOF.1.1C – 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.1.2C – 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.

Evaluator action elements:

AVA_SOF.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E – The evaluator shall confirm that the strength claims are correct.

AVA_VLA.1 Developer vulnerability analysis

Developer action elements:

AVA_VLA.1.1D – The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2D – The developer shall document the disposition of obvious vulnerabilities.

Content and presentation of evidence elements:

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

Evaluator action elements:

AVA_VLA.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E – The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

A typical attacker in the intended environment for the Bioscrypt™ Enterprise product is deemed to possess only limited knowledge of biometric systems and lack the skills and resources required to manipulate the Bioscrypt™ Enterprise Reader. Therefore, for an EAL2 level evaluation of Bioscrypt™ Enterprise, the strength of function to meet or exceed for AVA_SOF calculations is BASIC. The Bioscrypt™ Enterprise system, configured at this security level, has an FAR of less than 0.001 (1/1000) at a 95% confidence level. Any remaining vulnerabilities can be only be exploited by an attacker of moderate or high attack potential.

6.1 TOE SECURITY FUNCTIONS

A description of each of the TOE security functions follows.

F.ENROL The TOE provides users with the ability to enrol using fingerprint biometrics. The users are required to prove their identity by first authenticating with a valid NT password and username. The enrolment process generates a Bioscrypt™ template which includes a given user's biometric data. The biometric data undergoes a series of checks to ensure it is of sufficient quality to be used for authentication with a FAR of less than 0.001 (1/1000) at a 95% confidence level. A cryptographic key for the user is created by the BRC using a FIPS 186 pseudorandom number generator or an ANSI X9.17 standard pseudorandom number generator and either DES (56 bit key size) or two key Triple DES in CBC mode (112 bit key size) for the export or domestic versions of the TOE respectively.

F.BIODEL The TOE provides the ability to delete a user's Bioscrypt™ Collection (which contains the user's biometric data, cryptographic key, and password) using a command line function included with the GINA replacement. The user cryptographic key is deleted by being encrypted by the Bioscrypt™ Enterprise reader's key and then deleted (the user key can also be destroyed by overwriting the old key with a new key). This ability is restricted to a administrator who must authenticate using a biometric fingerprint before being granted the ability.

F.NEWBIO The TOE provides the ability to re-enrol a user. The re-enrol process requires that an administrator first delete the user's old Bioscrypt™ Collection, after which the user re-enrols as if it was the first time.

F.TRNFER The TOE can communicate between the BRC and Bioscrypt™ Database Service with confidentiality. Confidentiality for the Bioscrypt™ Template and user key is provided by two key Triple DES in CBC mode (112 bit key size). Confidentiality for the user's password is provided by DES (56 bit key size) or two key Triple DES in CBC mode (112 bit key size) depending on the export or domestic version of the TOE respectively.

F.BIOPRO The TOE protects the biometric data from unauthorised disclosure when stored through cryptographic means. The biometric data is stored as a part of the Bioscrypt™ Collection in the NT SAM database either locally in the case of a stand alone workstation, or on the PDC in the case of a NT domain. The Bioscrypt™ Collection is transferred and retrieved from the NT SAM database by the Bioscrypt™ Database Service. Confidentiality for the Bioscrypt™ Template and user key is provided by two key Triple DES in CBC mode (112 bit key size). Confidentiality for the user's password is provided by DES (56 bit key size) or two key Triple DES in CBC mode (112 bit key size) depending on the export or domestic version of the TOE respectively.

F.AUTH The TOE accurately authenticates a user to the underlying operating system using fingerprint biometrics and a username within a FAR of less than 0.001 (1/1000) at a 95% confidence level. The one exception is during enrolment where a password and username shall be used for authentication. Biometric authentication shall compare previously enrolled biometric data with new biometric data captured at the time of authentication. The new biometric data shall undergo a series of checks to ensure it is of sufficient quality to be used for authentication with a FAR of less than 0.001 (1/1000) at a 95% confidence level. Failed biometric authentication attempts terminate the login session before the user can perform any other action within the session and can also lockout the user account if specified by an administrator. The TOE does not biometrically authenticate a user who presents faked, copied or incorrect biometric data. Administrators must successfully authenticate before they can configure the GINA registry settings.

F.AUDIT The TOE generates an NT audit record for unsuccessful login attempts.

F.OBJREU The TOE zeroes any memory in the BER which stored biometric data, when the memory is de-allocated.

F.SESSION The TOE provides the ability to lock a user session both by the user themselves, and after a timeout period specified by an administrator (between 1 and 65535 seconds). The user must re-authenticate to un-lock the session. The TOE overwrites the display, and disables user access to data, devices, and

resources, preventing the user from performing any action except re-authenticating.

F.TOUT The TOE provides the ability to terminate a locked user session after a timeout period specified by an administrator (between 0 and 65535 seconds).

6.2 ASSURANCE MEASURES

A description of each of the TOE assurance measures follows.

M.ID The TOE incorporates a unique version identifier that can be displayed to the user.

M.CMLIST A list of all configuration items is maintained, and all configuration items are uniquely identified.

M.GETTOE The developer has a controlled process and procedures whereby the developer ships a shrink-wrapped copy of the TOE to a customer on CD-ROM. Both the process and procedures are documented.

M.SETUP The TOE includes an automated installation and setup program compatible with the TOE operating system. The installation process is self-explanatory, or provides additional instructions to clearly document the installation process. The default installation results in the secure installation and start-up of the TOE.

M.SPEC A high level, TOE design and functional specification have been provided by the developer for the evaluation which describes the TOE security functionality, subsystems, and interfaces.

M.TRACE Correspondence mappings are provided by the developer such that the security functionality detailed in the TOE functional specification is upwards traceable to this ST, and downwards traceable to the high level design.

M.DOCS Sufficient user and administrator guidance documentation are provided.

M.TEST A suitably configured TOE is tested in a controlled environment to confirm that TOE functionality operates as specified, and that the TOE is protected from a representative set of well-known attacks. A mapping between developer test cases and TOE functionality is provided by the developer. The assurance requirements also ensure the TOE functionality is tested in a real-world environment.

M.SECASS The developer examines the TOE design to ensure the security functions adequately address perceived threats in the security environment. The results of the examination are documented. Threats include deliberate attempts to disable, bypass, and brute-force attack the TSF.

7 PROTECTION PROFILE CLAIMS

This ST does not make compliance claims with respect to any Protection Profiles.

8 RATIONALE

8.1 SECURITY OBJECTIVES RATIONALE

8.1.1 OE Security Objectives Rationale

Table 3 provides a mapping of Security Objectives to Threats and Assumptions, and is followed by a discussion of how each is addressed by the corresponding Security Objectives.

Table 3 Mapping of Security Objectives to Threats and Assumptions

	T.SNIFF	T.REPLAY	T.FAKE	T.BIOTEMP	T.FVRFY	T.TOEATK	T.MODID	T.SHELL	T.UNDET	T.PASS	A.NOEVIL	A.TAMPER	A.PHYSEC	A.CHECK	T.USAGE	T.TROJAN	T.ENROL
O.FALPOS			X		X												
O.CRYPTO	X	X															
O.ACL						X	X			X							
O.USER															X		
O.AUDIT									X								
O.CLEAR				X													
O.LOCK								X									
O.EXCH	X																
O.GUIDAN											X				X	X	
O.VERIFY																	X
O.TAMPER												X					
O.PHYPRO						X							X	X			

T.SNIFF *A user may read a valid user's identification and authentication data as it is being transmitted between portions of the TOE or from where it is stored.*

O.CRYPTO and O.EXCH combine to provide protection against sniffing over all transmission paths.

T.REPLAY *An unauthorised user may capture valid user identification and authentication data, and use the identification and authentication data at a later time.*

O.CRYPTO prevents an attacker from capturing (and subsequently reusing) authentication data in a replay attack.

T.FAKE *A user may present a fake physiological sample or otherwise create an imitation of valid biometric data which is accepted as legitimate by the TOE.*

O.FALPOS prevents fake biometric data from being accepted as legitimate.

T.BIOTEMP *A user may obtain access to residual biometric data which was not cleared after use.*

O.CLEAR ensures no residual biometric data remains after operations have completed.

T.FVRFY *A individual may use their personal biometric data and be falsely verified as another valid user.*

O.FALPOS prevents biometric data from one user being accepted as another user's legitimate data.

T.TOEATK *A user may bypass, deactivate, or tamper with TOE hardware, firmware, or software.*

O.ACL prevents unauthorised users from tampering with the software. O.PHYPRO provides methods to prevent users from tampering with the hardware and firmware.

T.MODID *An unauthorised user may create, modify, or delete the identification and authentication data stored in the TOE.*

O.ACL prevents unauthorised users from altering authentication data.

T.SHELL *An individual may gain unauthorised access to another user's session after the user has been authenticated (e.g. after a valid user login).*

O.LOCK provides protection against unauthorised access to a user session.

T.UNDET *An individual's attempts to falsely authenticate as a valid user may go undetected.*

O.AUDIT generates audit records which can be used to detect failed logon attempts.

T.PASS *An individual may obtain a valid user's password and use the password to authenticate as the valid user.*

O.ACL provides biometric authentication preventing direct authentication using passwords (except during enrolment).

A.NOEVIL *Administrators are non-hostile and follow all administrator guidance; however, they are capable of error.*

O.GUIDANCE provides administrators with the guidance required to install, administer, and operate the TOE securely.

A.TAMPER *Authorised users are trusted not to tamper with the hardware (PC and biometric device).*

O.TAMPER asserts that authorised users will not tamper with the hardware (PC and biometric device).

A.PHYSEC *Unauthorised users are not allowed unattended physical access to the hardware (workstations, servers, PDCs, BDCs, and biometric device).*

O.PHYPRO prevents unauthorised users from tampering with the hardware.

A.CHECK *During enrolment the administrator will verify that the serial link has not been tampered with.*

O.PHYPRO prevents users from tampering with the serial link.

T.USAGE *The TOE may be configured, used and administered in an insecure manner.*

O.USER and O.GUIDANCE combine to provide users with the tools and guidance required to install, administer, and operate the TOE securely.

T.TROJAN *Compromise of the integrity and/or availability of the TOE may occur as a result of a TOE user unwittingly introducing a virus or trojan into the system.*

O.GUIDANCE provides users with guidance to avoid malicious code.

T.ENROL *An unauthorised user may enrol themselves as a valid user.*

O.VERIFY ensures users are properly identified during enrolment.

8.2 SECURITY REQUIREMENTS RATIONALE

8.2.1 Security Functional Requirements Rationale

Table 4 provides a mapping of Security Functional Requirements to Security Objectives, and is followed by a discussion of how each Security Objective is addressed by the corresponding Security Functional Requirements.

Table 4: Mapping of Security Functional Requirements to Security Objectives

	O.FALPOS	O.CRYPTO	O.ACL	O.USER	O.AUDIT	O.CLEAR	O.LOCK	O.EXCH	O.GUIDAN	O.VERIFY	O.TAMPER	O.PHYPRO
FAU_ADG.1					X							
FCS_CKM.1		X										
FCS_CKM.4		X										
FCS_COP.1		X										
FDP_ACC.2	X		X									
FDP_ACF.1	X		X									
FDP_RIP.1						X						
FIA_AFL.1			X									
FIA_ATD.1			X									
FIA_SOS.2	X											
FIA_UAU.2			X									
FIA_UAU.3	X		X									
FIA_UAU.5			X									
FIA_UID.2			X									
FIA_USB.1			X									
FMT_MSA.1			X	X								
FMT_MSA.2	X											
FMT_MTD.1				X								
FPT_ITC.1		X										
FPT_STP.1		X						X				
FTA_SSL.1							X					
FTA_SSL.2							X					
FTA_SSL.3							X					

O.FALPOS *The TOE must prevent faked or incorrect biometric data from being accepted as legitimate by the biometric device.*

FIA_UAU.3 provides protection against the biometric device accepting faked biometric data, or biometric data copied from another user. FIA_SOS.2, FMT_MSA.2 FDP_ACC.2, and FDP_ACF.1 combine to ensure good quality biometric data is generated initially and when used for verification (authentication). This serves to minimise the occurrences of incorrect biometric data being accepted as valid biometric data. Additionally, while not a Security Functional Requirement, AVA_SOF.1 helps ensure that the verification process is sufficiently “strong” enough to prevent false positives.

O.CRYPTO *The TOE must protect the confidentiality of the biometric data using encryption.*

FCS_CKM.1 and FCS_CKM.4 combine to define how cryptographic keys are generated and destroyed. FCS_COP.1 defines all the cryptographic operations which are performed by the TOE. FPT_ITC.1 and FPT_STP.1 define the transmission (Bioscrypt™ Database Service to NT SAM database, and BRC to Bioscrypt™ Database Service respectively) requirement for confidentiality.

O.ACL *The TOE must enforce access control such that only authorised users may create, modify and delete security attributes. Only biometric authentication will be allowed (excluding the enrolment process where password authentication is required).*

FIA_UAU.2 and FIA_UID.2 combine to prevent a user from performing any actions before authentication. FIA_UAU.3 ensures that unauthorised users cannot forge authentication information from other users. FIA_UAU.5 defines the rules which determine which authentication method will be used (password or biometric). FIA_AFL.1 defines the TOE behaviour in the event of authentication failure. FIA_USB.1 provides the binding between a user and the subject acting on their behalf within the TSC. FDP_ACC.2 defines the security policy for access control operations between all subjects and objects. FDP_ACF.1 and FIA_ATD.1 combine to define the security attributes required for authentication. FMT_MSA.1 defines the security policy for the management of security attributes.

O.USER *The TOE must provide functionality that enables users to effectively manage the TOE and its security functions from its human-machine interface (HMI).*

FMT_MSA.1 defines the security policy for the management of security attributes. FMT_MTD.1 defines the management of TSF data.

O.AUDIT *The TOE must generate a readable audit trail of security relevant events.*

FAU_ADG.1 defines the security relevant events for which an audit record is generated.

O.CLEAR *The TOE must ensure no residual or unprotected biometric data remains after operations are completed.*

FDP_RIP.1 ensures no residual biometric data is left within the TOE after operations are complete.

O.LOCK *The TOE must protect a user session against unauthorised access.*

FTA_SSL.1, FTA_SSL.2, and FTA_SSL.3 combine to ensure that a user session can be locked and terminated to prevent unauthorised access to the session.

O.EXCH *The TOE must exchange data between components of the TOE in a trusted manner.*

FPT_STP.1 defines the transmission requirement for confidentiality of data as it moves between the BRC and the Bioscrypt™ Database Service of the TOE.

O.GUIDAN *The users of the TOE must ensure that the TOE is delivered, installed, configured, administered, and operated in a manner that maintains its security.*

This objective is satisfied by non-IT environment security requirements that do not relate directly to the implementation of the TOE and are not included in the ST.

O.VERIFY *A method will exist such that all users' claimed identities will be reliably confirmed before enrolment.*

This objective is satisfied by non-IT environment security requirements that do not relate directly to the implementation of the TOE and are not included in the ST.

O.TAMPER *Authorised users do not tamper with the hardware (PC and biometric devices).*

This objective is satisfied by non-IT environment security requirements that do not relate directly to the implementation of the TOE and are not included in the ST.

O.PHYPRO *Controls and procedures must exist to prevent people from physically tampering with the TOE.*

This objective is satisfied by non-IT environment security requirements that do not relate directly to the implementation of the TOE and are not included in the ST.

8.2.2 Rationale for Explicitly Stated IT Security Requirements

FAU_ADG.1 FAU_ADG.1 is a modified form of FAU_GEN.1 from the CC part 2. The TOE relies on the underlying operating system to provide all audit functionality with the exception of the TOE generating audit records related to TSF. The TOE is the authentication mechanism for the underlying operating system and does not start or stop the auditing system, therefore the FAU_GEN.1 requirement was not applicable since it requires the TOE to audit the start-up and shutdown of the audit functions. The FAU_ADG.1 requirement is expressed and evaluated identical to FAU_GEN.1 minus bullet "a" of element FAU_GEN1.1 (start-up and shutdown of the audit functions).

FPT_STP.1 Data is transferred between components of the TOE in two places: between the BER and BRC, and between the BRC and Bioscrypt™ Database Service. Data protections is provided by the TOE for transfers between the BRC and Bioscrypt™ Database Service, however between the BER and BRC it is provided by an environmental security objective. Part 2 of the CC provides FPT_ITT for internal TSF data transfer protection but it requires that the TSF provide the protection in all cases, therefore FPT_STP.1 was created to address only a subset of internal TSF data transfer protection. FTP_STP.1 is expressed and evaluated identical to FPT_ITT.1 except that it applies to an assignment of separate TOE parts instead of "between separate parts of the TOE".

8.2.3 Assurance Requirements Rationale

The Bioscrypt™ Enterprise product is designed to provide biometric authentication for Windows NT systems. A typical attacker in the intended environment for the Bioscrypt™ Enterprise product is deemed to possess only limited knowledge of biometric systems and lack the skills and resources required to manipulate the Bioscrypt™ Enterprise reader. Therefore an assurance of EAL 2, structurally tested, was selected as the threat to security is considered to be unsophisticated attackers. It is felt that an evaluation at this level provides evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.

8.2.4 Rationale for Satisfying All Dependencies

Table 5 identifies the ST Security Functional Requirements and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency. For those cases where dependencies have not specifically been addressed, explanations of the rationale for excluding them are provided.

Table 5 Security Functional Requirement Dependencies

ST Requirement	Dependencies	Dependency Satisfied?
FAU_ ADG.1	FPT_STM.1	N
FCS_CKM.1	FCS_CKM.2 or [FCS_COP.1, FCS_CKM.4, & FMT_MSA.2]	Y
FCS_CKM.4	FDP_ITC.1 or [FCS_CKM.1 & FMT_MSA.2]	Y
FCS_COP.1	FDP_ITC.1 or [FCS_CKM.1, FCS_CKM.4, & FMT_MSA.2]	Y
FDP_ACC.2	FDP_ACF.1	Y
FDP_ACF.1	FDP_ACC.1 & FMT_ MSA.3	N
FDP_RIP.1	–	Y
FIA_AFL.1	FIA_UAU.1	Y (FIA_UAU.2 is hierarchical to FIA_UAU.1)
FIA_ATD.1	–	Y
FIA_SOS.2	–	Y
FIA_UAU.2	FIA_UID.1	Y (FIA_UID.2 is hierarchical to FIA_UID.1)
FIA_UAU.3	–	Y
FIA_UAU.5	–	Y
FIA_UID.2	–	Y
FIA_USB.1	FIA_ATD.1	Y
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] & FMT_SMR.1	N
FMT_MSA.2	ADV_SPM.1, [FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, & FMT_SMR.1	N
FMT_MTD.1	FMT_SMR.1	N
FPT_ITC.1	–	Y
FPT_STP.1	–	Y
FTA_SSL.1	FIA_UAU.1	Y (FIA_UAU.2 is hierarchical to FIA_UAU.1)
FTA_SSL.2	FIA_UAU.1	Y (FIA_UAU.2 is hierarchical to FIA_UAU.1)
FTA_SSL.3	--	Y

FAU_ADG.1 The dependency of FPT_STM.1 (Reliable time stamps) has not been met. The TOE generates log events which are sent to the underlying OS. Since the TOE relies on the underlying OS to provide the audit functionality, the FPT_STM.1 dependence is not required for this ST.

FDP_ACF.1 The dependency of FMT_MSA.3 (Static attribute initialisation) has not been met. The TOE does not provide any static attributes itself. Instead, attributes such as the initial username and password are set by an OS administrator outside of the TOE (in the environment). Therefore the dependence on FMT_MSA.3 is not required for this ST.

FMT_MSA.1 The dependency on FMT_SMR.1 (Security roles) has not been met. The TOE does not have any security roles; all users are treated the same for purposes of

authentication. Installation of the TOE, deletion of a Bioscrypt™ Collection, and creation of a new user account are all "privileged" operations associated with the TOE; however, these operations are performed by the OS administrators outside of the TOE (in the environment). Therefore the dependence on FMT_SMR.1 is not required for this ST.

FMT_MSA.2 The dependency on FMT_SMR.1 (Security roles) has not been met. The TOE does not have any security roles; all users are treated the same for purposes of authentication. Installation of the TOE, deletion of a Bioscrypt™ Collection, and creation of a new user account are all "privileged" operations associated with the TOE; however, these operations are performed by the OS administrators outside of the TOE (in the environment). Therefore the dependence on FMT_SMR.1 is not required for this ST. The dependency on ADV_SPM.1 has not been met. FMT_MSA.2 has a dependency on ADV_SPM.1 in order that secure values for security attributes be defined in the context of the TOE. This information is provided within the Bioscrypt™ Inc. documentation, and thus a complete security policy model is not required for this evaluation.

FMT_MTD.1 The dependency on FMT_SMR.1 (Security roles) has not been met. The TOE does not have any security roles; all users are treated the same for purposes of authentication. Installation of the TOE, deletion of a Bioscrypt™ Collection, and creation of a new user account are all "privileged" operations associated with the TOE; however, these operations are performed by the OS administrators outside of the TOE (in the environment). Therefore the dependence on FMT_SMR.1 is not required for this ST.

Table 6 : Assurance Requirement Dependancies

ST Requirement	Dependencies	Dependency Satisfied?
ACM_CAP.2	–	Y
ADO_DEL.1	–	Y
ADO_IGS.1	AGD_ADM.1	Y
ADV_FSP.1	ADV_RCR.1	Y
ADV_HLD.1	ADV_FSP.1	Y
	ADV_RCR.1	Y
ADV_RCR.1	–	Y
AGD_ADM.1	ADV_FSP.1	Y
AGD_USR.1	ADV_FSP.1	Y
ATE_COV.1	ADV_FSP	Y
	ATE_FUN.1	Y
ATE_FUN.1	–	Y
ATE_IND.2	ADV_FSP.1	Y
	AGD_ADM.1	Y
	AGD_USR.1	Y
	ATE_FUN.1	Y
AVA_SOF.1	ADV_FSP.1	Y
	ADV_HLD.1	Y
AVA_VLA.1	ADV_FSP.1	Y
	ADV_HLD.1	Y
	AGD_ADM.1	Y
	AGD_USR.1	Y

All dependencies for assurance components have been met.

8.2.5 Rationale for Security Functional Refinements

FIA_AFL.1 User Attribute Definition

Changed, “When the defined number of unsuccessful authentication attempts…” to “When the defined number of unsuccessful biometric authentication attempts…”. This was altered for clarity, but does not change the intent of FIA_AFL.1.

FCS_CKM.1 Cryptographic key generation

Changed “…shall generate cryptographic keys in accordance…” to “…shall generate cryptographic keys for the user in accordance…”. Added words to specify which version of the Bioscrypt™ Enterprise (export or domestic) uses each key type. The intent of FCS_CKM.1 has not been changed.

FCS_CKM.4 Cryptographic key destruction

Added the specific cryptographic keys for which each destruction method applies. The intent of FCS_CKM.4 has not been changed.

FCS_COP.1 Cryptographic operation

Added words to specify which version of the Bioscrypt™ Enterprise (export or domestic) uses each key type. The intent of FCS_COP.1 has not been changed.

FDP_ACF.1 Security attribute based access control

Added "…the following additional rules: before the assignment in FDP_ACF.1.4 to make it consistent with the other elements. The intent of FDP_ACF.1.4 has not been changed.

FDP_RIP.1 Subset residual information protection

Changed "The TSF shall ensure that any previous information content of a resource…" to "The TSF shall ensure that any previous information content of memory…" to better describe TOE functionality. The intent of FDP_RIP.1 has not been changed.

FTA_SSL.3 TSF-initiated termination

Changed "The TSF shall terminate an interactive session…" to "The TSF shall terminate a locked interactive session…" to better describe TOE functionality. The intent of FTA_SSL.3 has not been changed.

8.2.6 Rationale for Audit Exclusions

There are no audit exclusions for this ST therefore no rationale is required.

8.3 TOE SUMMARY SPECIFICATION RATIONALE

8.3.1 TOE Security Functions Rationale

Table 7 provides a mapping of Security Functions to Security Functional Requirements, and is followed by a discussion of how each Security Functional Requirement is addressed by the corresponding Security Function.

Table 7 Mapping of Security Functions to Security Functional Requirements

	FAU_ADG.1	FCS_CKM.1	FCS_CKM.4	FCS_COP.1	FDP_ACC.2	FDP_ACF.1	FDP_RIP.1	FIA_AFL.1	FIA_ATD.1	FIA_SOS.2	FIA_UAU.2	FIA_UAU.3	FIA_UAU.5	FIA_UID.2	FIA_USB.1	FMT_MSA.1	FMT_MSA.2	FMT_MTD.1	FPT_ITC.1	FPT_STP.1	FTA_SSL.1	FTA_SSL.2	FTA_SSL.3
F.ENROL		X			X	X			X	X					X	X	X						
F.BIODEL			X		X	X			X							X							
F.NEWBIO					X	X			X							X	X						
F.TRNFER				X																X			
F.BIOPRO				X															X				
F.AUTH					X	X		X	X	X	X	X	X	X	X			X					
F.AUDIT	X																						
F.OBJREU							X																
F.SESSION																					X	X	
F.TOUT																							X

FAU_ADG.1 *Audit data generation*

F.AUDIT satisfies the requirement for the generation of audit events for unsuccessful logins.

FCS_CKM.1 *Cryptographic key generation*

F.ENROL satisfies the requirement for the generation of cryptographic keys (DES 56bit key size or two key Triple DES in CBC mode 112bit key size depending on the export or domestic version of the TOE respectively) which are used to protect the confidentiality of the biometric data when stored, and during transmission between the BRC and Bioscrypt™ Database Service.

FCS_CKM.4 *Cryptographic key destruction*

F.BIODEL satisfies the requirement for the destruction of cryptographic keys (by overwriting the old key with a new key, or by being encrypted by the Bioscrypt™ Enterprise reader's key and then deleted), which are used to protect the confidentiality of the biometric data when stored, and during transmission between the BRC and Bioscrypt™ Database Service.

FCS_COP.1 *Cryptographic operation*

F.TRNFER and F.BIOPRO satisfy the requirement for the cryptographic operations (encryption/decryption of the user's password) which are used to

protect the confidentiality of the biometric data when stored, and during transmission between the BRC and Bioscrypt™ Database Service.

FDP_ACC.2 *Complete access control*

F.ENROL, F.BIODEL, F.NEWBIO, and F.AUTH combine to define all the operations between subjects and objects for which access control is enforced (there are no operations for which access control is not enforced). F.ENROL requires a user to authenticate using a username and password. F.BIODEL, F.NEWBIO and F.AUTH are administrator-only actions which require the administrator to authenticate using a username and biometric data.

FDP_ACF.1 *Security attribute access control*

F.ENROL requires a user to authenticate using a username and password. F.BIODEL, F.NEWBIO, and F.AUTH are administrator-only actions which require the administrator to authenticate using a username and biometric data. F.ENROL, F.BIODEL, F.NEWBIO, and F.AUTH combine to define all security attributes required for access control (username, password, and biometric data) and how they are used to enforce access control.

FDP_RIP.1 *Subset residual information protection*

F.OBJREU satisfies the requirement to prevent residual information being left behind after operations have completed in the BER.

FIA_AFL.1 *Authentication failure handling*

F.AUTH satisfies the requirement for terminating a login session if the user fails to authenticate.

FIA_ATD.1 *User attribute definition*

F.ENROL requires a user to authenticate using a username and password. F.BIODEL, F.NEWBIO, and F.AUTH are administrator-only actions which require the administrator to authenticate using a username and biometric data. F.ENROL, F.BIODEL, F.NEWBIO, and F.AUTH combine to define all security attributes required for access control (username, password, and biometric data)

FIA_SOS.2 *Generation of secrets*

F.ENROL generates the biometric data which is used later for comparison during biometric authentication. F.AUTH generates new biometric data which

is used for comparison against the previously enrolled biometric data during authentication. F.ENROL and F.AUTH satisfy the requirement that the TOE be able to generate biometric data be of sufficient quality to provide accurate authentication.

FIA_UAU.2 *User authentication before any action*

A user must be in an active user session to perform actions. F.AUTH will terminate a login session unless a user successfully authenticates using a username, and biometric data or password. F.AUTH satisfies the requirement for the authentication of a user before any action is performed on behalf of that user.

FIA_UAU.3 *Unforgeable authentication.*

F.AUTH satisfies the requirement that the TOE be able to prevent users from faking authentication data using a copy of authentication data. FIA_UAU.3 applies to both biometric data and NT password

Application note: Users are forced to authenticate using biometrics therefore can not use the NT password to authenticate directly. During enrolment, the process is monitored by an administrator (see O.VERIFY) to prevent a user from using another user's password and username.

FIA_UAU.5 *Multiple authentication mechanisms*

F.AUTH allows a user to authenticate using both biometric and password based authentication. F.AUTH satisfies the requirement for multiple authentication mechanisms.

FIA_UID.2 *User identification before any action*

A user must be in an active user session to perform actions. F.AUTH will terminate a login session unless a user successfully authenticates using a username, and biometric data or password. F.AUTH satisfies the requirement for the identification of a user before any action is performed on behalf of that user.

FIA_USB.1 *User-subject binding*

A session is bound to a user based their username and successful authentication during enrollment. F.ENROL and F.AUTH combine to satisfy the requirement for the binding of a user to a subject acting on behalf of the user within the TSC.

FMT_MSA.1 *Management of security attributes*

F.ENROL, F.BIODEL, and F.NEWBIO combine to satisfy the requirement for operations which involve the management of security attributes.

FMT_MSA.2 *Secure security attributes*

F.ENROL and F.NEWBIO combine to satisfy the requirement for operations where secure (quality) biometric data is generated for security attributes.

FMT_MTD.1 *Management of TSF data*

F.AUTH satisfies the requirement for managing which authentication mechanism (password or biometric) will be used.

FPT_ITC.1 *Inter-TSF confidentiality during transmission*

F.BIOPRO satisfies the requirement for confidentiality protection of the biometric data when stored by the Bioscrypt™ Database Service in the NT SAM database.

FPT_STP.1 *Subset Internal TSF data transfer protection*

F.TRNFER satisfies the requirement for confidentiality protection of the biometric data during the transmission of security related data between the BRC and the Bioscrypt™ Database Service.

FTA_SSL.1 *TSF-initiated session locking*

F.SESSION satisfies the requirement for session locking by the TSF.

FTA_SSL.2 *User-initiated locking*

F.SESSION satisfies the requirement for session locking by the user.

FTA_SSL.3 *TSF-initiated termination*

F.TOUT satisfies the requirement for the TSF to terminate a session after a specified period of time has expired.

8.3.2 TOE Assurance Measures Rationale

Table 8 provides a mapping of Assurance Measures to Assurance Requirements, and is followed by a short discussion of how the Assurance Requirements are addressed by the corresponding Assurance Measures.

Table 8 Mapping of Assurance Measures to Assurance Requirements

	ACM_CAP.2	ADO_DEL.1	ADO_IGS.1	ADV_FSP.1	ADV_HLD.1	ADV_RCR.1	AGD_ADM.1	AGD_USR.1	ATE_COV.1	ATE_FUN.1	ATE_IND.2	AVA_SOF.1	AVA_VLA.1
M.ID	X												
M.CMLIST	X												
M.GETTOE		X											
M.SETUP			X										
M.SPEC				X	X								
M.TRACE						X							
M.DOCS							X	X					
M.TEST									X	X	X		X
M.SECASS												X	X

ACM_CAP.2 *Configuration items*

M.ID and M.CMLIST combine to satisfy the requirement for configuration management by maintain a list of configuration items and providing unique id numbers to identify each item.

ADO_DEL.1 *Delivery procedures*

M.GETTOE satisfies the requirement for documented delivery procedures.

ADO_IGS.1 *Installation, generation, and start-up procedures*

M.SETUP satisfies the requirement for installation, generation, and start-up procedures.

ADV_FSP.1 *Informal functional specification*

M.SPEC satisfies the requirement for a functional specification.

ADV_HLD.1 *Descriptive high-level design*

M.SPEC satisfies the requirement for a high-level design specification.

ADV_RCR.1 *Informal correspondence demonstration*

M.TRACE satisfies the requirement for design specifications that are consistent throughout the documentation.

AGD_ADM.1 *Administrator guidance*

M.DOCS satisfies the requirement for administrator guidance documentation.

AGD_USR.1 *User guidance*

M.DOCS satisfies the requirement for user guidance documentation

ATE_COV.1 *Evidence of coverage*

M.TEST satisfies the requirement for evidence that all TOE security functions have been tested.

ATE_FUN.1 *Functional testing*

M.TEST satisfies the requirement for evidence that TOE security functions have been tested.

ATE_IND.2 *Independent testing – sample*

M.TEST satisfies the requirement for evidence that TOE security functions have been tested.

AVA_SOF.1 *Strength of TOE security function evaluation*

M.SECASS satisfies the requirement for evidence that all TOE security functions have been examined to ensure their strength against threats.

AVA_VLA.1 *Developer vulnerability analysis*

M.TEST and M.SECASS combine to satisfy the requirement for evidence that the TOE has been examined and tested in an effort to discover vulnerabilities.

9 ACRONYMS AND ABBREVIATIONS

Acronym	Definition
BDC	Backup Domain Controller (Windows NT)
BER	Bioscrypt™ Enterprise Reader
BRC	Biometric Reader Control
CBC	Cipher Block Chaining (mode of operation for Triple DES cryptography)
CC	Common Criteria for Information Technology Security Evaluation
DES	Data Encryption Standard
DLL	Dynamically Linked Library
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards (United States)
GINA	Graphical Identification aNd Authentication
HMI	Human Machine Interface
IT	Information Technology
OS	Operating System
PC	Personal Computer
PDC	Primary Domain Controller (Windows NT)
PP	Protection Profile
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy