Certification Report

EAL 2 Evaluation

Of

Bioscrypt™ Enterprise for NT Logon

Version 2.1.3

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

© 2001 Government of Canada, Communications Security Establishment

Evaluation number:	383-4-8
Version:	1.0
Date:	June 8, 2001
Pagination:	i to iv, 1 to 18

DISCLAIMER

The IT product identified in this certification report, and associated certificate, has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Evaluation and Certification Scheme using the Common Methodology for Information Technology Security Evaluation, Version 1.0, for conformance to the ISO 15408 Common Criteria for IT Security Evaluation, Version 2.1. This certification report, and associated certificate, applies only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and associated certificate, is not an endorsement of the IT product by the CSE or by any other organization that recognizes or gives effect to this report, and associated certificate. No warranty of the IT product by the CSE or by any other organization that recognizes or gives effect to this report, and associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (the Canadian CCS) provides a third-party evaluation service for determining the trustworthiness of IT security products. Evaluation is performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the Canadian CCS Certification Body (CB), managed by the Communications Security Establishment (CSE).

A CCEF is a commercial facility that has demonstrated the ability to meet the requirements of the Canadian CCS CB for approval to perform Common Criteria evaluations. A significant requirement for such approval by the Canadian CCS CB is accreditation to the requirements of the ISO Guide 17025: General requirements for the accreditation of calibration and testing laboratories. Accreditation is performed under the Program for the Accreditation of Laboratories Canada (PALCAN) administered by the Standards Council of Canada.

The CCEF that performed the evaluation of Bioscrypt™ Inc.'s Bioscrypt™ Enterprise for NT Logon product is EWA-Canada Ltd. located in Ottawa, Ontario, Canada.

By awarding a certificate, a certifying body asserts, to a degree of confidence commensurate with the Evaluation Assurance Level (EAL), that a product complies with the security requirements specified in its Security Target (ST). A ST is a requirement specification-like document that defines and scopes the evaluation activities. The consumer of certified IT products should review the ST, in addition to the Certification Report (CR), in order to gain an overall understanding of the product. This should specifically include any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (Evaluation Assurance Level) to which it is asserted that the product satisfies its security requirements.

The ST associated with this CR is identified by the following nomenclature:

Security Target for Bioscrypt™ Inc. Bioscrypt™ Enterprise for NT Logon
Version 2.1.3
EWA-Canada Document number: 1360-013-350
Version 3.2
Dated: 8 June 2001

This CR is associated with the Certificate of Product Evaluation dated 8 June 2001.

Windows NT is a registered trademark of Microsoft Corporation. Bioscrypt Enterprise for NT Logon is a trademark of Bioscrypt™ Inc.

Reproduction of this report is authorized, provided the report is reproduced in its entirety.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLE

EXECUTIVE SUMMARY

This Certification Report (CR) contains the results of the Common Criteria Evaluation Assurance Level 2 IT Security Evaluation for Bioscrypt™ Inc.'s Bioscrypt™ Enterprise for NT Logon Version 2.1.3 that was performed by EWA-Canada Ltd.

The evaluation was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (the Canadian CCS). The Canadian CCS has established a Certification Body (CB) that is managed by the Communications Security Establishment (CSE).

The information in this CR is fully substantiated and supported by the evidence contained in the applicable Evaluation Technical Report (ETR), an internal CCS document that contains proprietary design and analysis information.

The goal of this evaluation was to provide third-party security analysis and testing of the Bioscrypt™ Enterprise for NT Logon product. Bioscrypt™ Inc. sponsored the evaluation. The Common Criteria Evaluation Facility (CCEF) conducting the evaluation was EWA-Canada Ltd.

The evaluation activities consisted of a comprehensive suite of analysis and testing activities against the requirements of the Common Criteria for Information Technology Security Evaluation (CC) version 2.1, applied using the Common Methodology for Information Technology Security Evaluation (CEM) version 1.0. The CC is an ISO standard (ISO 15408) developed by the multinational Common Criteria Project sponsoring organizations.

The EWA-Canada Information Technology Security Evaluation and Testing (ITSET) facility informally tested five different developmental versions of the Bioscrypt™ Enterprise for NT Logon product as it evolved. The final evaluation version of the Bioscrypt™ Enterprise for NT Logon was Version 2.1.3, which includes both software and a serial-port biometric scanner. It was subjected to a comprehensive suite of documented formal tests during an intensive and fully planned four-month period. The applicable product and product development documentation was evaluated in accordance with the requirements of the CEM.

A comprehensive suite of security tests was run against the Bioscrypt™ Enterprise for NT Logon product both at the developer's facility and in the EWA-Canada ITSET lab.

The Bioscrypt™ Enterprise for NT Logon is a fingerprint biometric based authentication package for Windows NT. The package replaces the normal Windows graphical identification and authentication (GINA) library. This allows password authentication data to be retrieved and submitted to the GINA on behalf of the user by the product via a fingerprint template, referred to as the Bioscrypt™ Collection, that was created and stored through an enrollment process. Users authenticate by entering their username and then place their finger on the Bioscrypt™ Enterprise Reader. Bioscrypt™ Enterprise for

NT Logon compares the user's finger to the user's stored template, and if they match, opens a user session to the operating system (OS).

The product includes Data Encryption Standard (DES) and Triple-DES algorithms that have been tested and validated to the FIPS 46-3 and FIPS 81 data encryption standards by a Cryptographic Module Validation Program (CMVP) approved laboratory. The DES algorithms are used in the export version of the Biometric Reader Control (BRC) software and the Triple-DES algorithms are used in the domestic version of the BRC. Triple-DES only is used in the hardware/firmware for both domestic and export versions. A FIPS 140 validation was not performed on the Bioscrypt™ Enterprise for NT Logon product, and as such the ability of the cryptography to withstand a concerted attack is unknown.

The Bioscrypt™ Enterprise for NT Logon is designed as a self-contained, one-to-one trusted fingerprint authentication device. It provides a secure, trusted logon environment using fingerprint information instead of passwords. It is designed for high-end commercial grade security in markets such as finance, government, health and telecommunications.

The evaluation of the Bioscrypt™ Enterprise for NT Logon demonstrated that this security product conforms to the security functional requirements specified in the Security Target (ST), and that it is conformant to the Common Criteria assurance requirements for Evaluation Assurance Level 2 (EAL 2).

CSE, as the Canadian CCS Certification Body, declares that the Bioscrypt™ Enterprise for NT Logon Version 2.1.3 evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates (CCRA) and will be placed on the Certified Products List.

1 Identification of the target of evaluation

The Target of Evaluation (TOE) is Bioscrypt™ Enterprise for NT Logon Version 2.1.3 comprised of a Bioscrypt™ Enterprise Reader (BER), Biometric Reader Control (BRC) software and the Bioscrypt™ Biometric Windows graphical identification and authentication (GINA) library. A Bioscrypt™ Database Service is also required for distributed installations.

The exported version of the TOE uses both DES and Triple-DES algorithms in the cryptography. The domestic version of the TOE uses only Triple-DES algorithms in the cryptography. The manufacturer will ensure that the correct version of the product, either domestic or export is provided to the consumer when the product is purchased.

A typical Bioscrypt™ Enterprise set-up for a Microsoft Windows domain is shown in Figure 1.

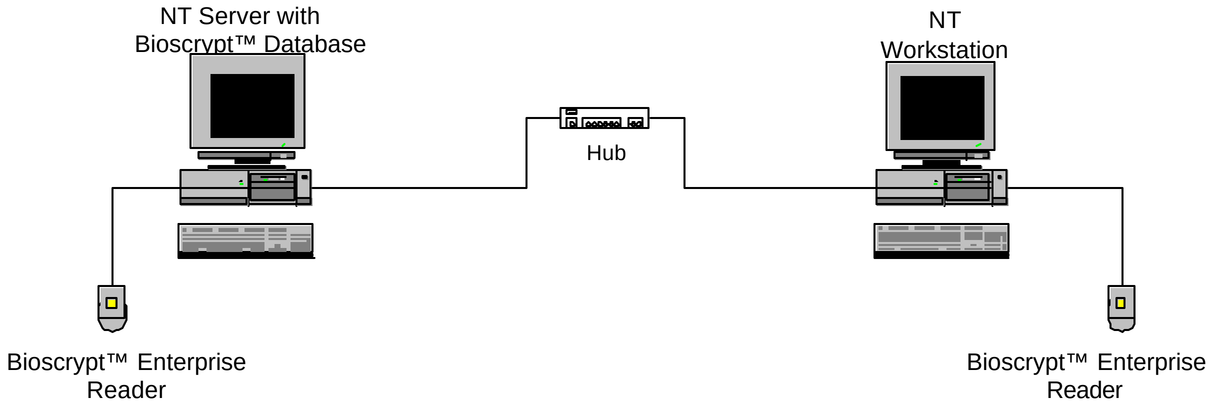
NT Server with Bioscrypt™ Database
NT Workstation
Hub
Bioscrypt™ Enterprise Reader
Bioscrypt™ Enterprise Reader

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

This product can also be configured in stand-alone mode where all major components are installed on the workstation itself. Section 1.2 of the Security Target (ST) describes this in further detail.

2 Security target

The Security Target (ST) associated with this Certification Report (CR) is identified by the following nomenclature:

Security Target for Bioscrypt™ Inc. Bioscrypt™ Enterprise for NT Logon
Version 2.1.3
EWA Document No. 1360-013-350
Version 3.2
Dated: 8 June 2001

3 Security policy

The Bioscrypt™ Enterprise for NT Logon product is a security product that enforces a security policy related to strong authentication, user identification and access control (in the context of logging on to the NT operating system).

After enrollment, the administrator can modify a register setting to enforce fingerprint authentication only. In such a case, a successful logon to the NT operating system can only be accomplished by a user typing in their valid username and presenting their fingerprint sample. Upon successful verification, the Bioscrypt™ Enterprise for NT Logon releases the standard NT password to the operating system and the user is granted access, completing the logon sequence.

If the username and fingerprint information does not match or are not valid, then the user's NT password is not released to the operating system and no access is granted. The user does not have the option of logging on by providing their username and password.

The Bioscrypt™ Enterprise for NT Logon technology protects the privacy of users' authentication credentials through encryption.

3.1 Bioscrypt™ Enterprise for NT Logon security functions

Bioscrypt™ Enterprise for NT Logon provides a large and comprehensive set of security functions. Table 1 summarizes the security functional requirements specified in the ST. This table includes two security functional requirements that are extensions to CC Part 2, namely FAU_ADG.1 – Audit data generation and FPT_STP.1 – Subset internal TSP data transfer protection.

Functional Components in the ST	
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

Functional Components in the ST	
Identifier	**Name**
FDP_ACF.1	Security attribute based 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 TSP data transfer protection
FTA_SSL.1	TSF initiated session locking
FTA_SSL.2	User initiated locking
FTA_SSL.3	TSF initiated termination

Table 1: Summary of security functional requirements

A brief listing of the specific security functions claimed by Bioscrypt™ Inc. in the ST is provided in the next sections.

3.2 Access control

There are five basic security functions related to access control that can be configured by the administrator. These are:

- Allow user choice of logging on using either a password or a fingerprint;
- Force user to log on with a fingerprint only;
- Provide the ability for an authorized user to change the user password (for the associated user account on the underlying OS) stored in the user's Bioscrypt™ Collection;
- Provide the ability to lock a user session both by the user, or after a timeout period specified by an administrator; and
- Provide the ability to terminate a user session after a timeout period specified by an administrator.

3.3 Audit

Bioscrypt™ Enterprise for NT Logon audits all failed attempts to log on to the system.

3.4 Data protection

Bioscrypt™ Enterprise for NT Logon protects biometric and authentication data from unauthorized disclosure when it is being stored or transmitted. It also zeroises any memory in the BER, which stores biometric data, when the data are no longer required.

4 Assumptions and clarification of scope

The assumptions about the product usage and environment settings should be considered by the consumer of this product as requirements for the product's installation and operating environment. They ensure proper functionality of the Bioscrypt™ Enterprise for NT Logon product as well as its ability to enforce the security policy.

4.1 Usage assumptions

If biometric authentication is required across a network (as opposed to the stand-alone configuration), the Bioscrypt™ Enterprise for NT Logon product must first be installed on the Primary Domain Controller (PDC). An NT System Administrator must do this.

4.2 Environmental assumptions

The environmental requirements and assumptions for this evaluation are:

- Bioscrypt™ Enterprise for NT Logon is physically located in a controlled access environment whereby unauthorized users are not allowed unattended physical access to the hardware (workstations, servers, PCs and BERs) to prevent unauthorized modifications to the product;
- Administrators are non-hostile and follow all administrator guidance; however, they are capable of error;
- Authorized users are trusted not to tamper with the hardware; and
- The administrator, who will personally verify the user's identity and that the serial link has not been tampered with, supervises the enrollment process.

4.3 External interfaces

Given the nature of the Bioscrypt™ Enterprise for NT Logon product, the only class of external interfaces that was evaluated is the human-machine interface between the user and the BER.

4.4 Definition of "users" and "administrators"

The term "user" refers only to individuals who use the product to log on to the system. The term "administrator" refers only to individuals who configure the Bioscrypt™ Enterprise for NT Logon product and perform specialized tasks.

4.5 Cryptography

Bioscrypt™ Enterprise for NT Logon secures data via cryptographic methods in three instances in the BER/BRC protocol:

- Creation of the Bioscrypt™ Collection in the BER always involves using Triple-DES for both the domestic and export versions to encrypt the fingerprint template along with a user key. The Bioscrypt™ Collection will be decrypted within the BER immediately prior to a verification attempt;
- The encryption and decryption in the BRC uses DES for the export version and Triple-DES for the domestic version; and

- There is link encryption (using Diffie-Hellman key exchange and El-Gamal public key encryption) between the BER and BRC components. The use of El Gamal for the protection of the transmitted DES or Triple-DES keys to prevent attacks that can be performed with knowledge of these keys implies that the attackers have an attack potential exceeding that which is commensurate with EAL2. As a result, a formal evaluation of the link encryption cryptography was beyond the scope of this evaluation.

Cryptographic keys for the user are randomly generated in accordance with the FIPS 186 standard for the export version, and in accordance with the ANSI X9.17 standard for the domestic of Bioscrypt™ Enterprise for NT Logon. However, cryptographic key generation was not tested as part of the evaluation, since cryptography is not the main focus of the product.

The DES and Triple-DES algorithms have been tested and validated to the FIPS 46-3 and FIPS 81 data encryption standards by a CMVP-approved laboratory. The DES/Triple-DES algorithms are used in the export /domestic versions of the BRC and the Triple-DES algorithms are used in both the domestic and export versions of the BER. A FIPS 140 validation was not performed on the Bioscrypt™ Enterprise for NT Logon product, and as such the ability of the cryptography to withstand a concerted attack is unknown.

5 Architectural information

5.1 Overview

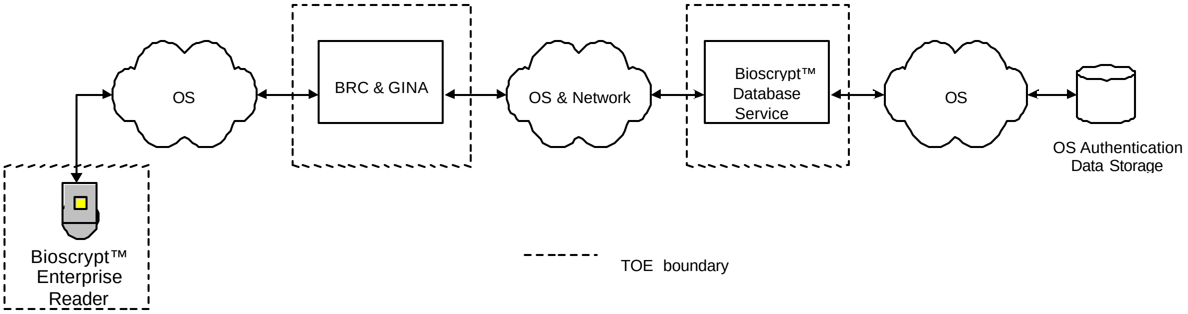
OS
BRC & GINA
OS & Network
Bioscrypt™ Database Service
OS
OS Authentication Data Storage
Bioscrypt™ Enterprise Reader
TOE boundary

Figure 2: TOE boundary diagram

The BER is a hardware device about the size of a mouse, which connects to a host PC via a serial link. The centre of the BER contains a sensor for scanning the fingerprint image. The BER contains a hard coded cryptographic key, which is set during manufacturing by Bioscrypt™ Inc. The customer can specify that a custom key should be configured, if desired. The BRC software is comprised of software libraries, which control the BER. The Bioscrypt™ Enterprise for NT Logon GINA is a replacement for the normal Microsoft GINA. The 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; however, a registry setting can be specified to force biometric authentication only. The evaluated configuration requires this registry setting on all users' PCs with the exception of any PCs required for enrollment and the PDC.

5.2 System requirements

The following are the minimum system requirements needed to support the operation of the Bioscrypt™ Enterprise for NT Logon product:

- Windows NT 4.0 Service Pack 4 or higher;
- Pentium 100 MHz or higher;
- 4 Mb free hard drive space; and
- 32 Mb RAM.

6 Evaluated configuration

The final evaluated version of the Bioscrypt™ Enterprise for NT Logon product is version 2.1.3 for either the domestic or export version. This product was installed as part of a Windows Domain running Windows NT 4.0 Service Pack 4. The evaluated configuration is the default configuration installed in accordance with the supplied guidance.

The major hardware components are a host PC or networked workstation with the Bioscrypt™ Enterprise Reader (BER) connected.

The major software components are:

- the BRC software version 2.1.0, which is analogous to a hardware device driver;
- the BER firmware version 2.1.3, which is required to operate the device;
- the NT GINA replacement for NT Logon version 2.1.0, which handles the interfaces with NT and the GUI; and
- the Bioscrypt™ Database service.

7 Documentation

The Bioscrypt™ Enterprise for NT Logon product comes with an electronic copy of the user manual, which serves as an installation and operating guide. The manual provides installation information, user guidance and administrator guidance.

8 Evaluation activities

The evaluation involved an analysis of Bioscrypt™ Inc.'s processes used to develop and support the Bioscrypt™ Enterprise for NT Logon product and associated documentation. The product documentation and design were considered from a security perspective, as were the associated operational user's manual and administrative guidance documentation.

8.1 Configuration management

The initial baseline version of the Bioscrypt™ Enterprise for NT Logon used for this evaluation was version 1.0. During the course of the evaluation, the product evolved through five different test versions. The product evolution was driven primarily by a combination of operational issues and the detailed CC security functional and assurance requirements that were necessary to pass the evaluation, although Bioscrypt™ Inc. took the opportunity to include additional product enhancements in these releases.

The final evaluation baseline is version 2.1.3 for both the domestic and export versions of the product.

The configuration management documents provided by Bioscrypt™ Inc. include a list of configuration items as well as a plan for maintaining management control of the product's hardware and software configuration.

8.2 Product delivery and operation

The Bioscrypt™ Enterprise for NT Logon product is purchased directly from the manufacturer, Bioscrypt™ Inc. Upon ordering, Bioscrypt™ Inc. will manufacture the BERs for the consumer's order and will set them up with the appropriate hard-coded cryptographic keys. The consumer receives the product as a package protected with tamper-evident seals. This ensures that interference with the product is detectable.

The Bioscrypt™ Enterprise for NT Logon product user manual provides online documentation outlining correct operating procedures, including the system requirements for a secure installation and start-up of the product. The administrator may choose to implement a number of configuration options to customize the use of the product at this time.

8.3 Development documentation

Bioscrypt™ Inc. provided all the necessary development documentation, which includes product specifications, design and requirement tracing.

8.4 Administrator and user guidance documentation

The Bioscrypt™ Enterprise for NT Logon product provides online administrator and user guidance documentation. The evaluated configuration of the Bioscrypt™ Enterprise for NT Logon product results from following the installation guidance without the requirement of any special instructions.

8.5 Testing

In addition to comprehensive testing that was performed by Bioscrypt™ Inc., a comprehensive suite of independent tests was developed and run by EWA-Canada on the product. Details can be found in Section 9 of this report.

8.6 Strength of function

Strength of function for a biometric device resolves to the False Match and False Non-Match rates of the product. The objective of the False Match rate testing is to verify Bioscrypt™ Inc.'s claims with respect to the rate with which the Bioscrypt™ Enterprise for NT Logon product incorrectly authenticates an attacker who is masquerading as a legitimate user. No False Non-Match rate was specified or claimed by Bioscrypt™ Inc. as it relates to convenience of use and is not security relevant for the product.

All testing was done to verify that the Bioscrypt™ Enterprise for NT Logon product would produce a False Match result no greater than 1 time in 1000, with a 95% statistical confidence interval.

A detailed analysis of Bioscrypt™ Inc.'s claims has been substantiated through analysis, testing and simulation.

8.7 Vulnerability assessment for the product

A comprehensive test suite was developed. Details can be found in section 9.6 of this report.

9 Product testing

9.1 Testing philosophy

In general there are three aspects to evaluation testing:

- assessing developer tests;
- performing independent tests; and
- performing penetration tests.

For this particular evaluation, the evaluators chose to develop a suite of independent tests by:

- examining the developer's test documentation;
- witnessing and sampling the developer tests;
- independently developing test documentation (e.g., test plan, test procedures, expected results); and
- conducting independent evaluator testing based on the evaluator test plans and procedures and documenting test results.

The test philosophy used in this evaluation was to test and evaluate the security features of the Bioscrypt™ Enterprise for NT Logon product, as scoped by the ST and described in the functional specification. In general, the philosophy used in the establishment of test procedures for the security evaluation of the Bioscrypt™ Enterprise for NT Logon product was to prove or disprove the security claims made by the vendor through positive- and negative- oriented "functional type" testing. Also, the evaluators tested for vulnerabilities and attempted to defeat the Bioscrypt™ Enterprise for NT Logon product through tampering and bypass testing based on defined attacks and vulnerabilities.

9.2 Testing coverage

EWA-Canada's approach to independently testing the Bioscrypt™ Enterprise for NT Logon product was to develop and document tests that covered all security requirements specified in the ST, with the exception of FCS_CKM.1 – Cryptographic key generation. Rigorous testing of a subset of security functionality (an approach compliant to the CEM) was appropriate for the following reasons:

- The Bioscrypt™ Enterprise for NT Logon product test documentation was comprehensive;

- It was efficient to observe Bioscrypt™ Inc.'s testing; and

- The Bioscrypt™ Inc.'s laboratory was more functionally capable than the EWA-Canada lab due to the availability of batch testing and simulation facilities.

The biometric relevant security functional and assurance requirements that were verified and validated through testing are grouped into the following four main areas:

- Major security functions of the Bioscrypt™ Enterprise for NT Logon product;

- False Match rate associated with the biometric device;

- Privacy of the captured and stored fingerprint template; and

- Environmental influences.

Resulting from this test coverage approach is the following list of test goals:

1. Test the delivery and installation procedures.
2. Test the BER device functions.
3. Test the BRC software functions.
4. Test the GINA software functions.
5. Test the security functions.
6. Test the password mechanisms.
7. Confirm the False Match claims.
8. Conduct the vulnerability testing in accordance with the security threats defined in the ST.
9. Confirm that standard NT security authentication attributes and functionality are still correct.
10. Test the password length.
11. Test the external interfaces.
12. Test the display of error codes and warnings.

9.3 Detailed test plan and procedures

EWA-Canada Ltd. provided comprehensive documentation of the configurations, detailed test goals, test objectives, test plans and detailed test procedures, along with the expected test results.

9.4 Conduct of the testing

EWA-Canada Ltd. informally tested several different developmental versions of the Bioscrypt™ Enterprise for NT Logon product to gain familiarity and to facilitate the evaluation planning process. The final evaluation version of the Bioscrypt™ Enterprise for NT Logon product was subjected to a comprehensive suite of formally documented tests during a four-month period at EWA-Canada Ltd's Ottawa laboratory. The actual test results were documented and were seen to correspond with the expected test results.

9.5 Cryptographic testing

The cryptographic testing was conducted under the requirements of the following documents:

a. The CCS Bulletin on Evaluation of Cryptography, April 2000; and

b. FIPS 46-3 and FIPS 81 data encryption standards.

It was mutually agreed upon by Bioscrypt™ Inc. and EWA-Canada to retain the services of Cygnacom Solutions as an accredited and CMVP-approved laboratory for the independent validation of the DES and Triple-DES algorithms.

Bioscrypt™ Inc. produced a toolkit for the instrumentation of the software and firmware to conduct the known test vector inputs and key injections to obtain the actual encrypted results. These tests were conducted at Bioscrypt™ Inc.'s facilities. The official test results on the final Bioscrypt™ Enterprise for NT Logon product were forwarded to the CMVP-approved laboratory for review/validation and forwarded to the National Institute of Standards and Technology (NIST) so that the certificate may be issued.

The CMVP-approved laboratory conducted the cryptographic validation comparison testing to the FIPS 46-3 and FIPS 81 data encryption standards. Regarding the validation of the cryptography, the DES and Triple-DES implementations for the product successfully passed the specified compliance tests, and appropriate certificates have been issued to attest to this fact.

9.6 Vulnerability testing

Vulnerability tests were conducted against the product to deal with the following types of scenarios and potential concerns:

- Compromising the symmetric keys in the BER hardware;
- Replay attacks against the serial link;
- False Match rate;
- Binary attacks to determine user passwords;
- Denials of service based on deletion of Bioscrypt™ Collections;
- Bypassing of the biometric logon;
- Reverse engineering of the BER firmware;
- BRC or BER memory exploitation of residual biometric information;
- Auto-population of GINA dialog boxes in software;
- Notification of invalid usernames;
- Stationary finger tests;

- Latent print tests;
- Impostor tests;
- Buffer overflow attacks against the GINA replacement software;
- Sniffing attacks;
- Fake finger tests;
- Residual file tests;
- Unauthorized modification of user credentials; and
- Ability to bypass account locking.

9.7 Testing results

For all formal tests, the actual results matched the expected results and confirmed that the security claims are as documented and the external interfaces of the product operate as claimed.

In summary, the independent testing by EWA-Canada Ltd. confirmed the following:

- All ST claims made by Bioscrypt™ Inc. that relate to the ability of the Bioscrypt™ Enterprise for NT Logon product to authenticate and control user access to the NT operating system were confirmed to be valid;
- The Bioscrypt™ Enterprise for NT Logon technology provides privacy protection for user information including fingerprints, passwords and logon authentication credentials;
- The product's use of the DES and Triple-DES algorithms was verified by algorithm validation under the CMVP, though a FIPS 140-1 validation was not performed;
- When properly installed and configured, the product improves upon and does not compromise the security of the Windows NT operating system;
- The False Match rate claimed by Bioscrypt™ Inc. is valid;
- The BER device is robust against imposter techniques and a wide variety of attacks as specified in Section 3.2 of the ST;
- There are no known residual vulnerabilities in the technologies that are exploitable in the intended environment; and

- The BER device provides effective suppression of latent fingerprint images as part of the automated image quality checks.

10 Results of the evaluation

The evaluation demonstrated that the Bioscrypt™ Enterprise for NT Logon product merits an Evaluation Assurance Level (EAL) 2 rating against the requirements of the Common Criteria (ISO 15408). The Bioscrypt™ Enterprise for NT Logon product meets the security requirements specified in the ST, which are CC Part 2 extended and CC Part 3 conformant to EAL 2.The evaluators found, and documented, compelling evidence that the Bioscrypt™ Enterprise for NT Logon product provides the claimed security protection.

11 Evaluator comments, observations and recommendations

11.1 Evaluator comments

The Bioscrypt™ Enterprise for NT Logon product is straightforward to configure, use and integrate into an NT environment.

The product documentation associated with the Bioscrypt™ Enterprise for NT Logon product was found to be of high quality in terms of completeness, level of detail, accuracy, usefulness and comprehensiveness.

11.2 Developer briefings

The developer briefings were extremely detailed and comprehensive with respect to the information presented on the product requirements, design and the corporate processes used to develop and support the product.

11.3 Recommendation

Corporate users looking for technology to include biometric authentication may wish to consider the Bioscrypt™ Enterprise for NT Logon product.

The product also provides the ability for the consumer to specify custom cryptographic keys for the BER, if desired. This allows for a high level of customization for a consumer's installation.

12 Abbreviations and acronyms

BER	Bioscrypt™ Enterprise Reader
BRC	Biometric Reader Control
CB	Certification Body
CC	Common Criteria for Information Technology Security Evaluation
CCEF	Common Criteria Evaluation Facility
CCRA	Arrangement on the Recognition of Common Criteria Certificates
CCS	Common Criteria Evaluation and Certification Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CMVP	Cryptographic Module Validation Program
CR	Certification Report
CSE	Communications Security Establishment
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
GINA	Graphical Identification and Authentication dynamic link library
GUI	Graphical User Interface
ISO	International Organisation for Standardisation
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NIST	National Institute of Standards and Technology
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories Canada
PDC	Primary Domain Controller
ST	Security Target
TOE	Target of Evaluation

13 References and bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

1. Common Criteria for Information Technology Security Evaluation, CCIMB-99-031/032/033, Version 2.1, August 1999
2. Common Methodology for Information Technology Security Evaluation, CEM-97/017, Part 1: Introduction and general model, Version 0.6, January 1997

3. Common Methodology for Information Technology Security Evaluation, CEM-99/008, Part 2: Evaluation and Methodology, Version 1.0, August 1999
4. CCS#4, Technical Oversight, Canadian Common Criteria Evaluation and Certification Scheme (CCS), Version 0.84, 13 April 2000
5. Security Target for Bioscrypt™ Inc. Bioscrypt™ Enterprise for NT Logon, 1360-013-350, Version 3.2, 8 June 2001
6. Evaluation Technical Report, 1360-370-D00, Version 1.1, 8 June 2001