AUSTRALASIAN INFORMATION SECURITY EVALUATION PROGRAM

Certification Report

Certificate Number: 2003/31

Iridian Technologies

KnoWho Authentication Server and Private ID

Issue 1.0
October 2003

Issued by:

Defence Signals Directorate - Australasian Certification Authority

EXECUTIVE SUMMARY

This report describes the findings of the evaluation of Iridian Technologies' KnoWho Authentication Server and Private ID software, to the Common Criteria (CC) Evaluation Assurance Level EAL2. It concludes that these products have met the target Assurance Level of CC EAL2. The evaluation was performed by LogicaCMG and was completed in August 2003.

Iridian KnoWho Authentication Server and Private ID software together with an iris image capture camera, form a biometric identification and verification product based on iris recognition technology, referred to in this report as the Iridian KnoWho Authentication Server.

The Australasian Certification Authority (ACA) provides recommendations in this report that are specific to the secure use of the Iridian KnoWho Authentication Server. In addition, clarification of the scope of evaluation is included and readers are informed of how to determine if the product is in its evaluated configuration.

Recommendations are provided on the following topics:

- Secure Usage,
- Secure Enrolment,
- Unique Private ID Station Keys,
- Residual Key Files on the KnoWho Server,
- Transaction Applications, and
- Protection of Target of Evaluation (TOE) Components.

This report has been written in accordance with the Common Criteria Recognition Arrangement and as such includes information about the underlying Security Polices of the product, the Architecture, and Analysis and Testing performed by the evaluators.

Ultimately, it is the responsibility of the user to ensure that the Iridian KnoWho Authentication Server meets their requirements. For this reason, it is ***strongly*** recommended that a prospective user of the product obtain the public version of the Security Target, and read this certification report thoroughly prior to deciding whether to purchase the product.

TABLE OF CONTENTS

Chapter 1 Introduction

Intended Audience

This certification report states the outcome of the IT security evaluation of Iridian Technologies' KnoWho biometric identification and verification product. It is intended to assist potential users when judging the suitability of the product for their particular requirements.

This report should be read in conjunction with the Security Target for Iridian KnoWho Authentication Server and Private ID (Ref [9]), which provides a full description of the security requirements and specifications that were used as the basis of the evaluation. A copy of the full Security Target may be requested from Iridian Technologies or Argus Solutions. The public version of the Security Target is available for download at http://www.dsd.gov.au.

Identification

The identification details for the evaluation are proved in Table 1 below.

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Iridian KnoWho Authentication Server v1.2.2, Private ID v2.1.15, LG IrisAccess 2200 Camera and Panasonic Authentication camera, Model BM-ET100US
Software Version	KnoWho Authentication Server v1.2.2 KnoWho Private ID v2.1.15
Security Target	KnoWho Authentication Server and Private ID Security Target version 2.18, September 2003
Protection Profile Claims	The Security Target does not claim conformance to any Protection Profiles.
Evaluation Level	CC EAL 2
Conformance Result	CC Part 2 Conformant CC Part 3 Conformant
Evaluation Technical Report	Evaluation Technical Report for KnoWho Authentication Server and Private ID, Issue 1.1 , September 2003.
Version of CC	CC Version 2.1, August 1999
Version of CEM	CEM-99/045 Version 1.0, August 1999
Sponsor	Argus Solutions
Developer	Iridian Technologies
Evaluation Facility	LogicaCMG
Certifiers	Katrina Johnson, Lachlan Turner, Aaron Doggett

Description of the TOE

The Target of Evaluation (TOE) is a biometric identification and verification product known as the 'Iridian KnoWho Authentication Server', and its primary role is to provide an organisation with the ability to perform identification and/or verification of individuals for access to IT assets according to their security needs.

The TOE architecture is based on a client-server model that is intended to integrate with transaction applications that provide connectivity between distributed parts of the TOE. The TOE consists of four distinct logical components:

- The **Authenticam** or **LG2200** biometric capture device, which takes a picture of an individual's iris from which an IrisCode will be generated.

- The **Iridian PrivateID Software** is image capture software that resides on the client PC. The primary function of this software is to capture images from the camera and select the best for transfer by a transaction application to the Iridian KnoWho Server. The PrivateID software will also include the nonce (issued by the KnoWho Server) with the selected image and protect the integrity of the iris image package by generating a Message Authentication Code (MAC). As part of the MAC generation, PrivateID encrypts the image data. The data is then passed to the client-side transaction application for transmission to the server-side transaction application on the KnoWho Server.

- The **Iridian KnoWho Server Software**, which will check the authenticity of the package by looking at the nonce within the package and verifying the integrity of the decrypted iris image data by regenerating the MAC associated with the package. Once the nonce and MAC are verified the received iris image data is encoded into a 512-byte IrisCode record. This IrisCode record is matched against the IrisCode templates residing in the KnoWho Database. For identification or verification, the KnoWho Server will pass the matching statistics, including a grant or deny decision, back to the requesting server-side of the transaction application for enforcement of the decision. For enrolment, the KnoWho Server will pass the decision to enrol or not to enrol the individual back to the enrolling server-side of the transaction application, and the enrolled identification number. The KnoWho Server interfaces with the KnoWho database that is used for the secure storage of the IrisCode templates and associated identification numbers, optionally along with the encrypted iris images, a user portrait image, the audit trail and configuration data for the TOE components.

- The **Iridian KnoWho Maintenance Application**, which is used by TOE Administrators as the means by which administrators manage the security features of the KnoWho Server.

For further information on the specific hardware and software components included in the evaluated configuration refer to Chapter 7: Evaluated Configuration, or the Security Target (Ref [9]).

Chapter 2 Security Policy

This section outlines the security policies and rules that the TOE must enforce, or comply with, for correct operation.

Organisational Security Policies

The TOE is designed to be operated in conjunction with the following Organisational Security Policies (OSPs) which must be defined by the owners of the TOE.

- ***P.Audit*:** Details of user activity will be recorded in an audit trail that must be preserved in accordance with relevant organisational archive requirements.

- ***P.Crypto*:** All cryptographic material is to be the subject of physical and technical controls as defined in the relevant National Authority Standards[1].

- ***P.Train*:** All individuals who access any security-related device must receive training on the proper use of the device as well as the security issues and vulnerabilities that may arise from its improper use. In particular, issues and vulnerabilities associated with secure enrolment of individuals must be included in such training.

- ***P.Biometric*:** The TOE must be used in a manner consistent with relevant National Authority policies[2] on the use of biometric devices for the intended biometric application.

- ***P.Roles*:** Organisational policy must define responsibilities for and assign individuals to the following roles:
    - *TOE Administrators*, who are responsible for the secure management and operation of the TOE, including operator enrolment and management of operator privilege, and management of TOE security-relevant data including configuration information;
    - *TOE Operators*, who are responsible for the enrolment of users and maintenance of user enrolments; and
    - *TOE Users*, who provide biometric samples to the TOE for identification, verification or enrolment.

  The organisational policy may allow two or more individuals to fulfil a single role; alternatively an individual may fulfil serval roles.

[1] Australian Communications-Electronic Security Instruction 33 (ACSI 33, Ref [4]) defines cryptographic standards for protection of non-national security information and includes guidance on key management.
[2] DSD does not provide specific policy on the use of biometric technologies, however, ASCI 33 (Ref [4]) provides the minimum standards for Australian government departments for logical access and physical access controls for IT systems and computer rooms.

TOE Security Policies

The TOE Security Policies (TSPs) define the security policies that the TOE must comply with in order to enforce the security functional requirements. The Security Target (Ref [9]) does not contain any explicit security policy statements, however, the TOE implements a number of implied TSPs, drawn from the collection of security functional requirements. The TOE has been found to implement the following TSPs:

- **Audit:** The TOE must generate audit records for security relevant events.
- **Cryptographic Support:** The TOE must provide cryptographic operations for protecting the confidentiality and integrity of information transmitted between separate parts of the TOE[3]. Cryptographic mechanisms must also protect IrisCodes and iris images stored in the biometric database from disclosure.
- **Identification and Authentication:** The TOE shall require identification and authentication of all users (TOE Administrators, TOE Operators, and TOE Users). The TOE must employ appropriate authentication mechanisms for the point of access to the TOE security functions (e.g. at the server or through a secure enrolment station).
- **Security Management:** The TOE must limit access to TOE security functions and associated data based on defined roles. The TOE maintains the roles of TOE Administrators, TOE Operators, and TOE Users.
- **Protection of the TOE Security Functions:** The TOE the must provide the following protective measures for TOE Security Functions:
  - Data used by the TOE security functions must be protected from disclosure and modification when it is transmitted between separate parts of the TOE, the TOE shall also detect and audit any such modification.
  - The TOE shall resist high-light level and low-light level optical based attacks against the biometric capture device.
  - The TOE must protect against replay attacks, the TOE shall also detect and audit any such attack.
  - The TOE must provide reliable time stamps for its own use.

[3] **Note:** It is important to note that the response to an authentication request is passed to the server-side component of the transaction application. It is the responsibility of the transaction application to protect the confidentiality and integrity of any authentication request response (accept / reject) passed over the network back to the requesting client application. See Chapter 9: Recommendations for transaction application.

Chapter 3 Intended Environment for the TOE

This chapter outlines the requirements and assumptions that govern the intended environment in which the TOE is designed to operate, and for which the TOE has been evaluated. In addition, this chapter clarifies the scope of the evaluation. Organisations wishing to implement the TOE in its evaluated configuration should review the evaluation scope to confirm that all the required functionality has been included in the evaluation, and must ensure that any assumed conditions are met in their operational environment.

Secure Usage Assumptions

The evaluation of the Iridian KnoWho Authentication Server took into account the following assumptions about the secure usage of the TOE:

- TOE administrators will follow all policies and procedures described in the TOE system documentation to ensure secure administration of the TOE.
- TOE Administrators and Operators are assumed to be non-hostile and trusted to perform all their duties in a competent manner.
- An appropriate source of cryptographic material, as defined by relevant National Authority Standards[4], to be used by the TOE must be available in the TOE environment.
- The TOE will be used for identifying, or verifying the identity of users for granting or denying access to IT assets protected by the TOE, e.g. Operating System resources, Network resources or application resources.
- It is assumed that strong physical security measures will be in place to prevent unauthorised physical access to the server components of the TOE.
- It is assumed that strong physical security measures will be in place to prevent unauthorised physical access to the secure enrolment stations used by the TOE.
- The underlying platform for the server components of the TOE will be configured to only accept connections from authorised TOE client components or other TOE server components.
- It is assumed that the TOE will be installed in a network that provides appropriate connectivity between components of the TOE, and that this interaction occurs through a transaction application.

[4] The assumption refers to the provision of Triple DES keys for use by the TOE. DSD does not provide specific policy on the generation of Triple DES keys, however, Chapter 9: Recommendations provides guidance specific to this product in regard to cryptographic keys.

Clarification of Scope

The scope of the evaluation is limited to those claims made in the Security Target (Ref [9]). All security related claims in the Security Target were evaluated by LogicaCMG during the evaluation. A summary of the Security Target is provided in Appendix A of this Certification Report. The evaluated configuration for the TOE is provided in Chapter 7: Evaluated Configuration.

The TOE provides the following evaluated security functionality:

- **Biometric Identification:** Acceptance of biometric samples provided by individuals and generation of IrisCodes for one-to-many (identification) comparison with stored biometric templates.

- **Biometric Verification:** Acceptance of biometric samples with an identification number, provided by individuals and generation of IrisCodes for one-to-one comparison with stored biometric templates.

- **Biometric Enrolment:** Creation of biometric templates and storage on the KnoWho server for subsequent use in identifying or verifying individuals, and deletion of biometric templates that are no longer required.

- **System Security Management:** Restriction of access to the functions for configuring the TOE security attributes to only authorised TOE Administrators.

- **Replay Detection and Prevention:** Detection of replayed transactions and forged data from the client PrivateID applications.

- **Forged Data Prevention:** Prevention of the use of forged biometric data subsequent to the enrolment process.

- **Security Audit:** Generation of audit records for security-relevant events.

- **Resistance to Physical Attack:** Resistance to high and low light optical-based attacks against the camera.

Potential users of the TOE are advised that the following **have not been evaluated** as part of the evaluation of the Iridian KnoWho Authentication Server:

- The client-side and server-side transaction applications. The client-side and server-side transaction applications request identification, verification or enrolment services from the TOE, and provide connectivity between distributed TOE components.

- The database management system and database that is used for the secure storage of the IrisCode templates and associated identification numbers, along with iris images, a user portrait image, the audit trail, and configuration data for the TOE components.

- Encryption functionality **other than** Triple DES. Triple DES is used for confidentiality of the iris image during transmission, Message Authentication Code generation and database confidentiality.

- Generation of Cryptographic Keys.

- APIs for the self enrolment of operators and users of the TOE.

- APIs for the self update and deletion of operator and users enrolled on the TOE.

- APIs for the retrieval of administrator, operator and/or user facial images.

The APIs identified above should be disabled through the maintenance application of the Iridian KnoWho Authentication Server during installation of the TOE.

Chapter 4 TOE Architecture

The TOE architecture is based on a client-server model that is intended to integrate with transaction applications that provide connectivity between distributed parts of the TOE and comprises two physically distinct components:

- The KnoWho server, comprising the Iridian KnoWho Server, KnoWho Biometric Database, and the Iridian KnoWho Maintenance Application; and
- The Verification or Enrolment Client, comprising the Iridian Private ID software and the LG2200 or Panasonic Authentication Camera.

These components integrate with transaction applications (external to the TOE) that provide the connectivity between the distributed parts of the TOE.

The TOE Security Functions (TSF) consists of the following four architectural components identified at the high level design. Each component implements a part of the security functionality. They are described as follows:

- **Image Capture Subsystem:** Provides functionality to capture and encrypt iris images for transmission to the KnoWho server for identification, verification or enrolment depending on the requirements of the client side of the transaction application.

TSF Subsystems forming the Matcher Core which are:

- **Encoder Subsystem:** Validates packages containing iris image data that has been collected by the Image Capture Subsystem located on a client verification or enrolment workstation. If a received data package contains a valid nonce, and the integrity of the data is successfully verified, the iris image is encoded into an IrisCode and the request is passed onto the Matcher Subsystem for further processing.
- **Matcher Subsystem:** Performs IrisCode matching for identification, verification or enrolment requests received via the Encoder Subsystem and provides responses to those requests.
- **Maintenance Subsystem:** Provides the functionality necessary for the configuration and management of the TOE. This subsystem is stated to physically reside on the KnoWho Server.

Chapter 5 Documentation

It is important that the Iridian KnoWho Authentication Server is used in accordance with the guidance documentation in order to ensure the secure usage of the TOE. The documents described in this chapter have been found to meet the requirements for Guidance Documentation specified by the Common Criteria EAL2 assurance level.

Iridian Technologies provides the following documents with the evaluated version of the product:

- KnoWho Authentication Server Installation Guide (Ref [12]),
- KnoWho Authentication Server Administrator's Manual (Ref [11]),
- KnoWho Authentication Server and Private ID Installation and Guidance Addendum (Ref [13]),
- Panasonic Authenticam Iris Recognition Camera Installation and Operation Guide for Windows 2000 Operating System (Ref [16]),
- PrivateID with LG2200 Imager: Hardware and Software Installation Guide for Windows 2000 (Ref [17]), and
- PrivateID with LG2200 Imager: Hardware and Software Installation Guide for Windows NT (Ref [18]).

The above documentation is intended to provide guidance and information required to install and configure the TOE in a secure manner.

Chapter 6 Analysis and Testing

The analysis and testing philosophy used in this evaluation was to test and evaluate the security features of the KnoWho product as scoped by the Security Target (Ref [9]), in accordance with the claimed assurance package. This chapter describes the following:

- **Strength of Function Analysis**: Analysis performed in validating the Strength of Function claims expressed as a False Accept Rate (FAR).
- **Functional testing:** Tests performed to ensure that the TOE operates according to its specification and is able to meet the requirements stated in the Security Target (Ref[9]).
- **Penetration testing:** Tests conducted to identify exploitable vulnerabilities in the TOE's intended operational environment.

Strength of Function Analysis

Central to the evaluation of biometric devices is the validation of the strength of function claims expressed as the specific metrics of a FAR. The FAR refers to the rate with which the Iridian KnoWho Authentication Server product incorrectly authenticates an attacker who is masquerading as a legitimate user. The FAR has direct implications on the security functionality of the TOE.[5]

In accordance with the rigour defined for the Evaluation Assurance Level claimed in the Security Target, EAL2, the evaluators performed an analysis of the underlying algorithms used in iris recognition technology in order to validate the FAR. Iridian has claimed a theoretical FAR of 1 in 1,100 000.

The analysis was performed in accordance with the strength of function analysis guidance provided in the CEM (Ref [8]). That is, the analysis assumes that the security function is implemented flawlessly and that the security function is used during attack within the limits of its design and implementation.

The evaluators studied the mathematical basis for the algorithm used to extract iris data reliably from a live video image and confirmed that there was sufficient degrees of freedom to enable biometric identification; supporting the assertion that iris recognition is a valid form of biometric identification.

The evaluators then examined the statistical decision theory used for recognising a given iris as belonging to a particular individual, and found all assertions to be valid. The ACA also conducted an assessment of the evidence provided for strength of function and also found the research and evidence to be valid.

The analysis showed that when implemented flawlessly, the algorithms used in the Iridian product would uphold the claimed FAR.

[5] The TOE's Strength of Function analysis also identifies the False Reject Rate (FRR). FRR refers to the product incorrectly denying authentication to a legitimate user. The FRR does not have a direct impact on the security functionality of the TOE and is not discussed further in this report.

Functional Testing

In this phase the evaluators analysed evidence of the developer's testing effort, performing the following:

- test coverage and depth analyses,
- test plans and procedures review, and
- review of expected and actual results.

In order to verify the developers testing effort, the evaluators developed a set of independent tests, comprising a sample of the developer tests as well as a selection of independent functional tests that expanded on the testing done by the developers.

By doing so, the evaluators were able to gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE.

The functions tested covered the full range of Security Functional Requirements identified in the Security Target (Ref [9]), with the exception of those that rely on cryptographic operations. Testing of the actual cryptographic processes is considered the responsibility of the national cryptographic authority. In Australia, the cryptographic functions have been evaluated by the Defence Signals Directorate, as the national authority, and found suitable for Australian and New Zealand Government use.

It was determined that the cost and level of effort required to perform bulk testing to validate the TOE's theoretical FAR was beyond the scope of the target level of assurance, EAL2. Therefore, the evaluators did not attempt to test and verify the FAR claim of 1 in 1,100,000. However, the ACA is satisfied that the developers and evaluators conducted a testing effort that is commensurate with EAL2 and did not experience a false acceptance.

Penetration Testing

The developers performed a vulnerability analysis of the TOE in order to identify any obvious vulnerabilities in the product and to show that they are not exploitable in the intended environment for the TOE. This analysis included a search for possible vulnerability sources in the following:

- evaluation deliverables,
- intended TOE environment,
- public domain sources, and
- internal Iridian Technologies sources.

A number of potential vulnerabilities relevant to the product type were identified and in each case the developers were able to show that the vulnerability was not exploitable in the intended environment.

Based on the information given in the developer's vulnerability analysis, the evaluators were able to devise a penetration test plan that would test that the TOE is resistant to penetration attacks performed by an attacker with low attack potential, exploiting any of the identified vulnerabilities. In addition, the evaluators performed an independent vulnerability analysis in order to identify any possible vulnerabilities that had not been addressed by the developers. Based on this information, the evaluators identified further independent penetration tests.

Upon completion of the penetration testing activity, the evaluators concluded that the TOE did not display any susceptibility to vulnerabilities obtained from the developer or those from the evaluators' independent vulnerability analysis.

The penetration testing effort did however identify the biometric enrolment process as a potential point of attack. The identified vulnerabilities are not exploitable in the TOE's intended operating environment; however, it should be noted that the TOE relies on procedural security in order to protect against attackers exploiting inherent vulnerabilities in the TOE. Section 9 of this report provides recommendations for the secure use of the TOE in its intended operating environment.

Chapter 7 Evaluated Configuration

This chapter describes the evaluated configuration of the TOE and also provides procedures for determining the evaluated version of the TOE.

The TOE is comprised of the components included in Table 2 below.

Table 2: Evaluated TOE Components

Physical TOE Components	Hardware/Software Platforms
Panasonic Authenticam	Model BM-ET100US
LG IrisAccess 2200	Model 2200
Iridian PrivateID for Panasonic Authenticam PrivateID v2.1.15	Operating Systems: • Windows 98 2nd Edition; or • Windows Me; or • Windows 2000. Recommended Hardware Configuration: • Pentium 333MHz PC; • 64Mb RAM; • USB Port; • Network Interface Card; • Hard Drive with sufficient capacity to store software; and • CD-ROM Drive for installation.
Iridian PrivateID for LG2200 PrivateID v2.1.15	Operating Systems: • Windows 98 2nd Edition; or • Windows NT4.0 Workstation SP5; or • Windows 2000 SP 1 Recommended Hardware Configuration: • Pentium 233MHz PC; • 64Mb RAM; • VGX FrameGrabber Card; • Available Serial Port; • Network Interface Card; • Hard Drive with sufficient capacity to store software; and • CD-ROM Drive for installation.
Iridian KnoWho Authentication Server Iridian KnoWho Authentication Server Version 1.2.2 Iridian Maintenance Application	Operating Systems: • Windows NT 4.0 Server Service Pack 5 or • Windows 2000 Server or Advanced Server with Service Pack 1 RBDMS Software (Can be installed on a separate server): • Oracle 8.1.5, 8.1.6 or 8.1.7; or • Microsoft SQL Server 7.0; or • Microsoft SQL Server 2000.

	Recommended hardware configuration: • Dual Processor Pentium II 400 MHz; • 256Mb RAM; • RAID 5 Configuration; • 9Gb Ultra-Wide SCSI HDD, average seek time 9ms, average latency 3ms; and • CD-ROM Drive for installation.

Procedures for Determining the Evaluated Version of the TOE

When placing an order for the Iridian KnoWho Authentication Server, purchasers should make it clear to their supplier that they wish to receive the evaluated product. They should then receive the correct software and documentation to allow them to configure the product in accordance with the evaluated configuration.

The KnoWho Authentication Server and PrivateID Installation and Administrator Guidance Addendum (Ref [13]) provides instructions for configuring the TOE so that it is in its evaluated configuration.

TOE users can confirm that they are running the evaluated version of the TOE by checking that they are running the software versions listed in Table 2 above, and by confirming that the TOE is configured as described in the KnoWho Authentication Server and PrivateID Installation and Administrator Guidance Addendum (Ref [13]).

Chapter 8 Results Of The Evaluation

Evaluation Procedures

The evaluation of the Iridian KnoWho Authentication Server was conducted using the Common Criteria for Information Technology Security Evaluation (Refs [5] to [8]), under the procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [1], [2], [14] and [15]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [3]) were also upheld during the evaluation and certification of this product.

Certification Result

The Australasian Certification Authority has determined that Iridian KnoWho Authentication Server and PrivateID upholds the claims made in the Security Target (Ref [9]) and has met the requirements of the Common Criteria EAL2 assurance level.

Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability that exploitable vulnerabilities remain undiscovered.

Common Criteria EAL2

EAL2 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation and the high-level design of the TOE, to understand the security behaviour.

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

EAL2 also provides assurance through a configuration list for the TOE, and evidence of secure delivery procedures. A detailed explanation of the assurance requirements for EAL2 can be found in part 3 of the Common Criteria (Ref [7]).

Chapter 9 Recommendations

The following recommendations include both information from the evaluators that has been highlighted throughout the course of the evaluation as well as the activities performed by the certifiers in regards to the evaluation deliverables provided by the developer.

Secure Usage

It is recommended that those responsible for the TOE address all secure usage assumptions and security requirements for the non-IT environment provided in the Security Target (see Chapter 3: Intended Environment for a list of the secure usage assumptions and Appendix A: Security Target information for a list of the security requirements for the non-IT environment). The TOE must be installed and configured in accordance with the KnoWho Authentication Server and Private ID Installation and Administrator Guidance Addendum (Ref [13]).

Secure Enrolment

It is recommended that those responsible for the TOE ensure that adequate processes and procedures and physical security protection mechanisms are in place to ensure the enrolment process is only performed in a supervised and controlled manner. See section 4.2 'Adding a New Enrolment' of the KnoWho Authentication Server and Private ID Installation and Administrator Guidance Addendum (Ref [13]) for specific guidance on this topic.

Unique Private ID Station Keys

The Iridian KnoWho Authentication Server utilises symmetric encryption to cryptographically protect requests sent from Private ID clients to the KnoWho Authentication Server. In order to perform this function, each Private ID client has a Triple DES encryption key associated with it known as the Private ID Station Key. This key is stored locally on the client and also recorded in the KnoWho Database.

Purchasers of the TOE should be aware that Private ID ships with a non-unique default Station Key. In order to receive a unique Private ID Station Key, purchasers must inform their reseller that they wish to use a unique Private ID Station Key for their implementation.

It is therefore highly recommended that in accordance with section 3.2 of the KnoWho Authentication Server and Private ID Installation and Administrator Guidance Addendum (Ref [13]), purchasers of the TOE inform their reseller that they wish to use a unique Private ID Station Key within their implementation.

Where a unique Private ID Station Key implementation is requested, purchasers of the TOE should ensure that appropriate measures are taken to protect unauthorised disclosure of the issued Private ID Station Key whilst it is in transit from the issuing body.

Residual Key Files on the KnoWho Server

On the KnoWho Authentication Server, Station Keys and the Database Encryption Key are loaded through the Maintenance Application as documented in the KnoWho Authentication Server Administrator's Guide (Ref [11]).

Users of the TOE should be aware that when the Private ID Station Keys and Database Encryption Key are loaded into the KnoWho Database via the Maintenance Application, the key files used in this process are not automatically deleted from the server machine.

Once Station Keys and the Database Encryption Key have been loaded, it is recommended that all key files be removed from the local machine and stored in a secure environment or securely deleted.

Transaction Application

Users of the TOE must be aware that the Iridian KnoWho Authentication Server does not include a Transaction Application, which will be required in normal operation to request identification, verification or enrolment services from the TOE. It is recommended that, where possible, the TOE be installed in an environment where the Transaction Application has been evaluated to at lease the same level of assurance as the TOE.

The Transaction Application should provide adequate protection for the communication of authentication data between its server and client components. It is important to note that the response to an authentication request is passed to the server-side component of the Transaction Application. It is the responsibility of the Transaction Application to protect the confidentiality and integrity of any authentication request response (accept / reject) communicated over the network back to the requesting client application.

It is also recommended that the server-side component of the Transaction Application be installed on the same host as the KnoWho Authentication Server. Where this is not possible, the confidentiality and integrity of the data passed between the KnoWho Authentication Server and the server-side component of the Transaction Application should be protected.

Protection of TOE Components

It is recommended that the KnoWho Authentication Server and Secure Enrolment Stations be provided with adequate physical protection mechanisms to ensure that unauthorised users are not able to gain physical access to key components of the TOE.

It is also recommended that the underlying platform for the Iridian KnoWho Authentication Server be configured to only accept connections from authorised TOE client components or other authorised server components. The TOE should be installed in a network infrastructure that provides adequate protection and isolation from uncontrolled logical access.

Appendix A Security Target Information

A brief summary of the Security Target (Ref [9]) is given below. Potential customers should obtain the public version of the Security Target (available at http://www.dsd.gov.au) and review it before purchasing the KnoWho product. A copy of the full Security Target may be requested from Iridian Technologies or from Argus Solutions.

Security Objectives for the TOE

KnoWho has the following security objectives:

- The TOE shall provide the means to identify or verify individuals for access to IT assets, which is consistent with the organisational security policy P.BIOMETRIC[6], and measured by the false acceptance rates (FAR) and false rejection rates (FRR) for the TOE.

- The TOE shall limit access to, TOE security functions by individual on the basis of:
    - Their allocated role; and
    - The functions that are assigned that role.

  In accordance with the roles policy (P.ROLES).

- The TOE shall provide the means of preventing forgery of authentication data sent to the KnoWho Server. This includes two-dimensional forgeries of biometric samples and 'replay' attacks.

- The TOE shall resist optical-based physical attacks against the biometric capture device of the TOE.

- The TOE shall record necessary events to ensure that all users of the TOE are held accountable for their actions.

Security Objectives for the Environment

KnoWho has the following security objectives on the environment in which it exists:

- Those responsible for the TOE shall ensure that procedures and/or mechanisms are in place to ensure that generation, storages and handling of cryptographic material is conducted in accordance with the rules defined by the organisational security policy P.CRYPTO.

- Those responsible for the TOE shall ensure that procedures and/or mechanisms are in place to ensure that logical access to the TOE server components is appropriately controlled.

[6] Refer to Chapter 2: Security Policy for all Organisational Security Policy definitions

- Those responsible for the TOE shall ensure that procedures and/or mechanisms are in place to ensure that physical access to the TOE server components, and the secure enrolment stations, is appropriately controlled.

- Those responsible for the security of the organisation shall provide initial and ongoing training for all individuals, not just Administrators. This training should include security awareness of vulnerabilities, in particular, those associated with enrolment. In addition, those responsible for the security of the organisation shall ensure that all appropriate background checks, psychological assessments, and security clearances, as required, are conducted for all TOE Administrators and TOE Operators.

- Those responsible for the TOE shall ensure that procedures and/or mechanisms are in place to ensure that network connectivity between distributed parts of the TOE, and that this interaction occurs through a transaction application.

Threats

The following threats are addressed by the TOE:

- An impostor may make a zero effort forgery attempt to impersonate an authorised user of the TOE to gain access to the IT assets protected by the TOE.

- An impostor may use a forged two-dimensional iris image (e.g. an image produced from a high resolution photograph) for an authorised user to gain access to the IT assets protected by the TOE.

- An impostor may direct an attack against a similar biometric template for an authorised user to gain access to the IT assets protected by the TOE.

- An impostor uses a residual biometric image from a previous user to gain access to the IT assets protected by the TOE.

- An impostor may direct an attack against a noisy or null image to gain access to the IT assets protected by the TOE.

- An unauthorised user attempts to illegally enrol on the biometric system in order to gain access to the IT assets protected by the TOE.

- A user attempts to exceed their privilege on the biometric system to gain unauthorised access to the IT assets protected by the TOE.

- An attacker attempts to modify the configuration of the TOE or security relevant data such as the user security attributes (e.g. stored in the enrolled images database) to gain access to the IT assets protected by the TOE.

- An attacker may attempt to mount a network-based attack against the TOE security functions, which succeeds without detection.

- An attacker floods the biometric system with noise data attempting to cause improper operation of the capture device causing an individual to be erroneously allowed or denied entry to the IT assets protected by the TOE.

Summary of the TOE Security Functional Requirements

The KnoWho SFRs are given below. Full description of these SFRs can be found in Section 5.1 of the Security Target (Ref [9]).

- Class FAU: Audit
  - FAU_GEN.1 Audit data generation
- Class FCS: Cryptographic Support
  - FCS_COP.1 Cryptographic Operation
- Class FIA: Identification and Authentication
  - FIA_ATD.1 User attribute definition
  - FIA_UAU.2 User authentication before any action
  - FIA_UAU.3 Unforgeable authentication
  - FIA_UAU.5 Multiple authentication mechanisms
  - FIA_UAU.7 Protected authentication feedback
  - FIA_UID.2 User identification before any action
- Class FMT: Security Management
  - FMT_MOF.1 Management of security functions behaviour
  - FMT_MTD.1 Management of TSF Data
  - FMT_SMF.1 Specification of Management Functions
  - FMT_SMR.1 Security Roles
- Class FPT: Protection of TSF Functions
  - FPT_ITT.1 Basic internal TSF data integrity monitoring
  - FPT_ITT.3 TSF data integrity monitoring
  - FPT_PHP.3 Resistance to physical attack
  - FPT_RPL.1 Replay protection
  - FPT_STM.1 Reliable time stamps

Security Requirements for the IT environment

The TOE has the following requirements for the IT environment:

- Class FCS: Cryptographic Support
  - FCS_CKM.1 Cryptographic key generation

Security Requirements for the Non-IT Environment

The TOE has the following security requirements for the Non-IT environment:

- **KnoWho Server is to be physically protected –** The KnoWho Server shall be located within a controlled access facility that will prevent unauthorised physical access.

- **Secure enrolment stations are to be physically protected –** The client PC used for enrolment shall be located within a controlled access facility that will prevent unauthorised physical access.

- **Iridian KnoWho Server administrators, operators and users are well-trained according to their role –** The TOE environment shall ensure that administrators are trained and motivated to make the right choices when providing administrative support to the TOE, and that operators and users are trained and motivated to operate and use the TOE in a secure fashion.

- **Procedures for the management of cryptographic material in accordance with national authority standards –** The TOE environment shall ensure that at all times cryptographic material is stored and handled in accordance with the national authority standards.

- **Controlled Administrator Access to core TOE components –** The TOE environment shall provide procedures for installing, configuring and maintaining the underlying operating system for each of the core TOE components such that access is limited to only authorised administrators. These core components consist of KnoWho server, database systems and secure enrolment stations, but exclude client workstations. For example, accounts on the core TOE component platforms should only exist for authorised administrators.

- **Configuration of infrastructure –** The TOE environment shall provide procedures and guidance for TOE Administrators to ensure that the infrastructure surrounding and supporting the TOE is installed, configured and maintained correctly, and that connectivity is provided between distributed TOE components via transaction applications. For example, procedures and guidance on configuring the TCP/IP ports available on the KnoWho Server.

Appendix B Acronyms

ACA	Australasian Certification Authority
ACSI	Australian Communications – Electronic Security Instruction
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
API	Application Programming Interface
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
COM	Common Object Model
CSP	Cryptographic Service Provider
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FAR	False Accept Rate
FRR	False Reject Rate
MAC	Message Authentication Code
PP	Protection Profile
RDBMS	Remote Database Management System
SFP	Security Function Policy
SFR	Security Functional Requirements
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

Appendix C References

[1] AISEP Publication No.1- Description of the AISEP
AP 1, Version 2.0, February 2001
Defence Signals Directorate

[2] AISEP Publication No.2 - The Licensing of the AISEFs
AP 2, Version 2.1, February 2001
Defence Signals Directorate

[3] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security
May 2000

[4] Australian Communications - Electronic Security Instruction 33
Defence Signals Directorate
http://www.dsd.gov.au

[5] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC)
Version 2.1, August 1999, CCIMB-99-031

[6] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements (CC)
Version 2.1, August 1999, CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements (CC)
Version 2.1, August 1999, CCIMB-99-033

[8] Common Methodology for Information Technology Security Evaluation (CEM) Part 2.
Version 1.0, August 1999, CEM-99/045

[9] Iridian KnoWho Authentication Server and Private ID Security Target
Document Version 2.18, September 2003
Iridian Technologies

[10] Iridian KnoWho Authentication Server and Private ID Evaluation Technical Report (ETR)
Issue 1.1, September 2003
LogicaCMG
(EVALUATION-IN-CONFIDENCE)

[11] KnoWho Authentication Server Administrator's Manual
Revision D, April 2002
Iridian Technologies

[12] KnoWho Authentication Server Installation Guide
Revision D, April 2002
Iridian Technologies

[13] KnoWho Authentication Server and Private ID Installation and Guidance Addendum
Version 1.7, August 2003
90East

[14] Manual of Computer Security Evaluation Part I - Evaluation Procedures
EM 4, Issue 1.0, April 1995
Defence Signals Directorate
(EVALUATION-IN-CONFIDENCE)

[15] Manual of Computer Security Evaluations Part II - Evaluation Tools and Techniques
EM 5, Issue 1.0, April 1995
Defence Signals Directorate
(EVALUATION-IN-CONFIDENCE)

[16] Panasonic Authenticam Iris Recognition Camera Installation and Operation Guide for Windows 2000 Operating System
Revision A, September 2001
Iridian Technologies

[17] PrivateID with LG2200 Imager: Hardware and Software Installation Guide for Windows 2000
Revision A, March 2002
Iridian Technologies

[18] PrivateID with LG2200 Imager: Hardware and Software Installation Guide for Windows NT
Revision A, March 2002
Iridian Technologies