KnoWho Authentication Server and Private ID

Security Target

Version 2.18

September 2003

Prepared for:

Argus Solutions Ltd
Level 10
55 Lavender St Sydney NSW 2061
Australia

www.argus-solutions.com

and

Iridian Technologies
1245 Church St, Suite 3
Moorestown NJ 08057
USA

www.iridiantech.com

Document Control	Written by	Checked by	Approved by
Name	John Bluhdorn	Peter Lilley	Peter Lilley
Title	Security Consultant	Manager Professional Services Group	Manager Professional Services Group

Version Number	Version Date	Change Details
1.0	27 June 2001	Initial release
2.0	15 August 2001	Updated with additional information from Iris Australia and Iridian Technologies.
2.5	3 October 2001	AISEP Entry Release.
2.6	9 November 2001	Updated to resolve EORs
2.7	25 February 2002	Updated to resolve EORs
2.8	23 May 2002	Updated to resolve EORs, and add LG2200 camera
2.9	31 May 2002	Updated to resolve EORs
2.10	28 June 2002	Updated deliverables references and for evaluator comments
2.11	07 August 2002	Updated deliverables references and for evaluator comments
2.12	21 August 2002	Updated to add PrivateID encryption functionality
2.13	26 September 2002	Updated to resolve EORs
2.14	29 October 2002	Updated to refine claims
2.15	06 December 2002	Updated to refine claims
2.16	10 December 2002	Updated to refine FIA_UAU.3 claims
2.17	14 July 2003	Updated to resolve final EORs
2.18	03 September 2003	Updated to resolve final EOR

Document Reference
90East PSG Document Reference Number: 03/239

Document Classification

Trademarks

"KnoWho™" is a trademark of Iridian Technologies Inc.
"Authenticam™" is a trademark of Iridian Technologies Inc.
"PrivateID™" is a trademark of Iridian Technologies Inc.
"IrisCode™" is a trademark of Iridian Technologies Inc.
"LG 2200" is a trademark of LG Electronics Inc.

Company Titles

Within this document, the following shortened forms of company titles may be used:

Argus Solutions Pty Ltd	- 'Argus'.
Iridian Technologies Inc	– 'Iridian'.
90East (Asia Pacific) Pty Ltd	– '90East'.

Table of Contents

Conventions and Terminology 1

CONVENTIONS 1

TERMINOLOGY 1

REFERENCES 4

Document Organisation 5

1 Introduction 6

1.1 ST AND TOE IDENTIFICATION 6

1.2 SECURITY TARGET OVERVIEW 6

1.3 COMMON CRITERIA CONFORMANCE 8

2 TOE Description 9

2.1 OVERVIEW OF THE TOE 9

2.2 PHYSICAL SCOPE OF THE TOE 13

2.3 SECURITY FEATURES 15

2.4 FEATURES OUTSIDE OF SCOPE 16

3 TOE Security Environment 17

3.1 SECURE USAGE ASSUMPTIONS 17

3.2 THREATS TO SECURITY 18

3.3 ORGANISATIONAL SECURITY POLICIES 19

4 Security Objectives 20

4.1 SECURITY OBJECTIVES FOR THE TOE 20

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT 21

5 IT Security Requirements 22

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 22

5.2 TOE SECURITY ASSURANCE REQUIREMENTS 30

5.3 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT 37

5.4 SECURITY REQUIREMENTS FOR THE NON-IT ENVIRONMENT 38

6 TOE Summary Specification 40

6.1 SECURITY FUNCTIONS 40

6.2 ASSURANCE MEASURES 45

7 PP Claims 48

8 Rationale 49

8.1 SECURITY OBJECTIVES RATIONALE 49

8.2 SECURITY REQUIREMENTS RATIONALE 56
8.3 TOE SUMMARY SPECIFICATION RATIONALE 64
8.4 RATIONALE FOR EXTENSIONS 74
8.5 PP CLAIMS RATIONALE 75
Appendix A - Acronyms 76

List of Tables

TABLE 1: PHYSICAL COMPONENTS OF THE TOE 13
TABLE 2: SUMMARY OF TOE SECURITY FEATURES 15
TABLE 3: ASSUMPTIONS 17
TABLE 4:THREATS ADDRESSED BY THE TOE 18
TABLE 5: THREATS ADDRESSED BY THE OPERATING ENVIRONMENT 18
TABLE 6: ORGANISATIONAL SECURITY POLICIES 19
TABLE 7: SECURITY OBJECTIVES FOR THE TOE 20
TABLE 8: SECURITY OBJECTIVES FOR THE ENVIRONMENT 21
TABLE 9: TOE SECURITY FUNCTIONAL REQUIREMENTS 22
TABLE 10: TOE SECURITY ASSURANCE REQUIREMENTS 30
TABLE 11: IT SECURITY FUNCTIONS 40
TABLE 12: ASSURANCE MEASURES 45
TABLE 13: MAPPING OF THREATS, ASSUMPTIONS AND OSPS TO SECURITY OBJECTIVES 49
TABLE 14: MAPPING OF SECURITY OBJECTIVES TO THREATS, POLICIES AND ASSUMPTIONS 51
TABLE 15: SUFFICIENCY OF SECURITY OBJECTIVES 52
TABLE 16: MAPPING OF SECURITY OBJECTIVES TO SECURITY REQUIREMENTS 56
TABLE 17: MAPPING OF SECURITY REQUIREMENTS TO SECURITY OBJECTIVES 56
TABLE 18: SUFFICIENCY OF SECURITY REQUIREMENTS 58
TABLE 19: DEPENDENCY ANALYSIS 62
TABLE 20: MAPPING OF SFRS TO IT SECURITY FUNCTIONS 64
TABLE 21: MAPPING OF IT SECURITY FUNCTIONS TO SFRS 66
TABLE 22: SUITABILITY OF IT SECURITY FUNCTIONS 68
TABLE 23: MAPPING OF SARS TO ASSURANCE MEASURES 73

List of Figures

FIGURE 1: EXAMPLE APPLICATION FOR KNOWHO SERVER AND PRIVATE ID 12

Conventions and Terminology

Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 2.1 of the Common Criteria [CC]. Selected presentation choices are discussed here to aid the Security Target reader. The CC allows several operations to be performed on functional and assurance requirements. The allowable operations defined in paragraph 2.1.4 of Part 2 of the CC [CC2] are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets, i.e. [assignment_value(s)].
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *underlined italicised* text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the CC an iteration number inside parenthesis, for example, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.

All operations described above are used in this Security Target. *Italicised text* is used for both official document titles and text meant to be emphasised more than plain text.

Terminology

The terminology used in the Security Target is that defined in the Common Criteria [CC1, CC2]. The following additional TOE specific terminology is included to assist the consumer of the Security Target:

Attempt	The submission of a biometric sample to a biometric system for identification or verification. A biometric system may allow more than one attempt to identify or verify an enrolee.
Biometric	A measurable, physical characteristic or personal behavioural used to recognise the identity, or verify the claimed identity of an enrolee.

Biometric Application The use to which a biometric system is put.

Biometric Data The extracted information taken from the biometric sample and used either to build a reference template or to compare against a previously created reference template.

Biometric Sample Data representing a biometric characteristic of an end-user that was captured by a biometric system.

Biometric System An automated system capable of:

a) capturing a biometric sample from an end-user;

b) extracting biometric data from that sample;

c) comparing the biometric data with that contained in one or more reference templates;

d) deciding how well captured biometric data matches with reference templates; and

e) indicating whether or not an identification or verification of identity has been achieved.

Capture The method of taking a biometric sample.

Identification Number The system-assigned unique identifier associated with a biometric template.

Comparison The process of comparing a biometric sample with a previously stored reference template or templates.

Enrolee A person who has a biometric reference template stored within the biometric system.

Enrolment The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity within the biometric system.

False Acceptance The incorrect identification of an individual or incorrect verification of an impostor by a biometric system against a stored biometric reference template.

False Acceptance Rate (FAR). The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The FAR is stated as follows:

FAR = NFA/NIIA

or

FAR = NFA/NIVA where,

FAR is the false acceptance rate

NFA is the number of false acceptances

NIIA is the number of impostor identification attempts

NIVA is the number of impostor verification attempts

False Rejection When a biometric system fails to identify an enrolee or fails to verify the legitimate claimed identity of an enrolee.

False Rejection Rate (FRR). The probability that a biometric system will fail to identify an enrolee, or verify the legitimate claimed identity of an enrolee. The FRR is stated as follows:

FRR = NFR/NEIA

or

FRR = NFR/NEVA where,

FRR is the false rejection rate

NFR is the number of false rejections

NEIA is the number of enrolee identification attempts

NEVA is the number of enrolee verification attempts

Goat A biometric system end-user whose pattern of activity when interfacing with the system varies beyond the specified range allowed by the system, and who consequently may be falsely rejected by the system.

Identification/Identify The one-to-many process of comparing a submitted biometric sample against all of the biometric reference templates stored within the biometric system to determine whether it matches any of the templates and, if so, the identity of the enrolee whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity amongst the database rather than verify a claimed identity. This is in contrast to verification.

Impostor A person who submits a biometric sample in either an intentional or inadvertent attempt to be identified or verified as another person who is an enrolee.

IrisCode®	A 512-byte code generated by passing a captured Iris image through the proprietary Daugman algorithm that is used by the Iridian KnoWho™ Server as the basis for identifying and/or verifying an individual
Nonce	A time value parameter, such as a counter or a time stamp that is used no more than once for the same purpose in cryptography to prevent (undetectable) replay attacks.
Template	Data that represents the biometric measurement of an enrolee used by the biometric system for comparison against subsequently submitted biometric samples.
Threshold	The value above which a biometric data is accepted and equal to or below which a biometric data is rejected. The value is adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric application.
Transaction Application	A client-server application that uses identification, verification and/or enrolment services of the TOE. Normally, separate client-side and server-side transaction components will communicate with each other, and with the Application Programming Interface (API) of the appropriate TOE component, i.e. the Private ID API on the client system, and the KnoWho Authentication Server API on the server system.
Verification/Verify	The process of comparing a submitted biometric sample against the biometric reference template of a single enrolee whose identity is being claimed, to determine whether it matches the enrolee's template. This is in contrast to identification.
Zero Effort Forgery	An arbitrary attack on a specific enrolee identity in which the impostor masquerades as the claimed enrolee using his or her own biometric sample.

References

[3DES] Federal Information Processing Standard (FIPS) Publication 46-3, Data Encryption Standard, 25 October 1999.

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999.

[CC1] Common Criteria Part 1: Introduction and General Model, Version 2.1, CCIMB-99-031, August 1999.

[CC2] Common Criteria Part 2: Security Functional Requirements, Version 2.1, CCIMB-99-032, August 1999.

[CC3] Common Criteria Part 3: Security Assurance Requirements, Version 2.1, CCIMB-99-033, August 1999.

Document Organisation

Section 1 provides the introductory material for the Security Target.

Section 2 provides general purpose and TOE description.

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

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

Section 5 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3 [CC2, CC3], respectively, which must be satisfied by the TOE.

Section 6 identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Section 7 makes any protection profile claims applicable to the TOE.

Section 8 provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Next, Section 8 provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the protection profile requirements.

Appendix A documents an acronym list to define frequently used acronyms applicable to the TOE.

1 Introduction

This introductory section presents *security target (ST)* identification information and an overview of the ST structure. A brief discussion of the ST development methodology is also provided.

1.1 ST and TOE Identification

This section provides information needed to identify and control this ST and its Target of Evaluation (TOE). This ST targets an **Evaluation Assurance Level (EAL) 2** level of assurance for the TOE.

ST Title:	KnoWho Authentication Server and Private ID Security Target, Version 2.16
TOE Identification:	Iridian KnoWho™ Authentication Server v1.2.2, Private ID™ v2.1.15, LG IrisAccess™ 2200 camera and Panasonic Authenticam™ camera, Model BM-ET100US
CC Version:	Common Criteria for Information Technology Security Evaluation, Version 2.1 Final
ST Evaluation:	Australasian Information Security Evaluation Program, Defence Signals Directorate, Australian Department of Defence
Author(s):	Peter Lilley, Anne Robins
Keywords:	Biometric, Iris Recognition, Identification, Verification

1.2 Security Target Overview

The Iridian KnoWho Authentication Server and Private ID software, together with an iris image capture camera, which may be either the Panasonic Authenticam camera (referred to as 'Authenticam') or the LG2200 IrisAccess camera (referred to as 'LG2200'), form a biometric identification and verification product (the TOE), based on iris recognition technology, that provides an organisation with the flexibility to perform identification and/or verification of individuals for access to the IT assets according to their security needs. Identification seeks to answer the question "Who is the individual?" by attempting to match the supplied biometric sample of an individual with any one of the set of enrolled biometric templates (a one-to-many process). Verification seeks to answer the question of "Is the individual who they claim they are?" by attempting to match the supplied biometric sample with a single claimed biometric template (a one-to-one process) referenced by an identification number.

The TOE architecture is based on a client-server model that is intended to integrate with transaction applications that provide connectivity between the PrivateID and the camera installed on a client workstation and the KnoWho Server. When invoked by a transaction application, the PrivateID software captures a series of digital images of the subject's eye through the camera. Image metrics within the PrivateID software inspect the images for sufficient quality and iris content. Once a suitable image has been acquired, an audible signal is generated and a message is displayed to indicate that the image capture process has been successful or if a timeout has occurred. The captured image is then encrypted, and a message integrity component is added before being made available to the client-side of the transaction application for transmission to the KnoWho server via the server-side of the transaction application.

The KnoWho Server accepts the iris image captured by the PrivateID software, decrypts the image data and confirms the image integrity, generates an IrisCode from the supplied image, and then performs either verification (one to one matching) or identification (one to many matching) as required by the server-side transaction application. The IrisCode is generated for use in the matching process against the IrisCode templates located within the KnoWho Database. If the individual's biometric sample matches with a biometric template stored within the database, the individual has been identified and/or verified. Conversely, if an individual's biometric sample does not match with a biometric template stored within the database, the individual has not been identified and/or verified.

In each case, KnoWho server results are returned to the requesting transaction application. The transaction application may, in turn, be acting as part of a larger organisational application, which could use the KnoWho server information to determine whether or not access to IT resources will or will not be granted.

In order to be identified or verified by the KnoWho Server, an individual must first be enrolled by the organisation. During enrolment, the camera takes a series of pictures of one or both of an individual's irises with each passed through to the Private ID software that resides on a client PC. As in the identification process suitable images are selected and sent, via the transaction application, to the KnoWho Server where an IrisCode is generated for each iris, and sent to the KnoWho Database for secure storage.

The KnoWho Database stores at least one IrisCode with the individual's identification number, and optionally, one or more iris images.

The KnoWho Server stores limited personal data, by indexing a stored encrypted IrisCode template, and optionally the associated encrypted iris image, with an identification number. IrisCodes and any associated iris image records are not available to the requesting client and server-side transaction applications that transmit the iris image (from the PrivateID software) to the KnoWho Server, and are securely stored within the KnoWho Database.

To support secure operation, the TOE provides functionality to audit all security-relevant events appropriate to the biometric application, and all biometric audit data is securely stored within KnoWho Database, accessible only by the administrator. Additionally, for secure management, the TOE includes a Maintenance Application accessible only by administrators, which provides functionality for management of keys, passwords and server parameters, and privilege management.

The TOE provides a number of countermeasures to prevent the introduction and use of two-dimensional forged biometric images, such as photographs and drawings of eyes. These countermeasures are implemented through the mutual support of several TOE components. The camera will record only images of sufficient clarity, the PrivateID software will select only images which meet minimum quality and iris content requirements, and the KnoWho server will only accept data from the client within the limited timeframe imposed through the use of a timeout on the data acquisition process.

In summary, the TOE enables organisations to set and enforce access control policies based on a physiological biometric ('something you are') rather than the traditional use of passwords ('something you know') and/or tokens ('something you have').

1.3 Common Criteria Conformance

The TOE is conformant with Part 2 of the CC, version 2.1 [CC2] and the assurance requirements of EAL 2 as defined in Part 3 of the CC, version 2.1 [CC3].

2 TOE Description

This section provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Overview of the TOE

This section presents an overview of the Iridian KnoWho Server, PrivateID, and LG2200 or Authenticam biometric system, known as the TOE, to assist potential users in determining whether it meets their 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, and consists of *four* distinct logical components:

- The **Authenticam** or **LG2200** biometric capture device (referred to as 'the camera'), which takes pictures 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 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, Private ID 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 source 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 now matched against the IrisCode templates residing in the KnoWho Database. For identification or verification, the KnoWho Server will pass matching statistics back to the requesting server-side of the transaction application so that a decision to grant or deny access can be made. For enrolment, the KnoWho Server will pass the decision to enrol or not 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, along with the 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 the TOE Administrators as the means by which administrators manage the security features of the KnoWho Server.

The camera, PrivateID and the KnoWho Server allow an organisation to enforce security policies for the control of access to IT resources through the use of the unique physiological features of an individual's iris pattern. The TOE uses an individual's iris pattern taken by the camera using the PrivateID software and sends this through to the KnoWho Server, which will generate a unique IrisCode, which is compared against the KnoWho Database, as the biometric sample for identification and/or verification.

The TOE provides an organisation with the flexibility to perform identification and/or verification of individuals for access to the IT assets protected by the TOE according to their security needs. Identification seeks to answer the question "Who is the individual?" by attempting to match the supplied IrisCode of an individual with any one of the enrolled biometric template IrisCodes (a one-to-many process). Verification seeks to answer the question of "Is the individual who they claim they to be?" by attempting to match the supplied IrisCode with a single claimed biometric template IrisCode (a one-to-one process) referenced by an identification number.

IrisCodes provide a highly accurate means of identifying and/or verifying individuals. An individual's iris pattern is formed through the random tearing of tissue during the first year of human life, remains stable throughout their entire life and is not genetically determined. Therefore, once the tearing process is complete an individual's iris patterns are different for their left and right eyes. Further, given that the tearing process is not genetically determined, the iris patterns for identical twins are different, providing a physiological characteristic superior to DNA as a basis for biometric recognition.

The TOE generates IrisCode templates for individuals through enrolment, which subsequently generates an identification number, and sends the IrisCodes to the KnowWho Database server for secure storage. Importantly, the Iridian KnoWho Server attempts to match the IrisCode with any other IrisCode stored within the KnoWho Database before accepting the enrolment, thus preventing an individual from having several enrolled identities within the TOE. The KnoWho server provides a response to the server-side of the transaction application on the success or failure of the enrolment and the generated identification number.

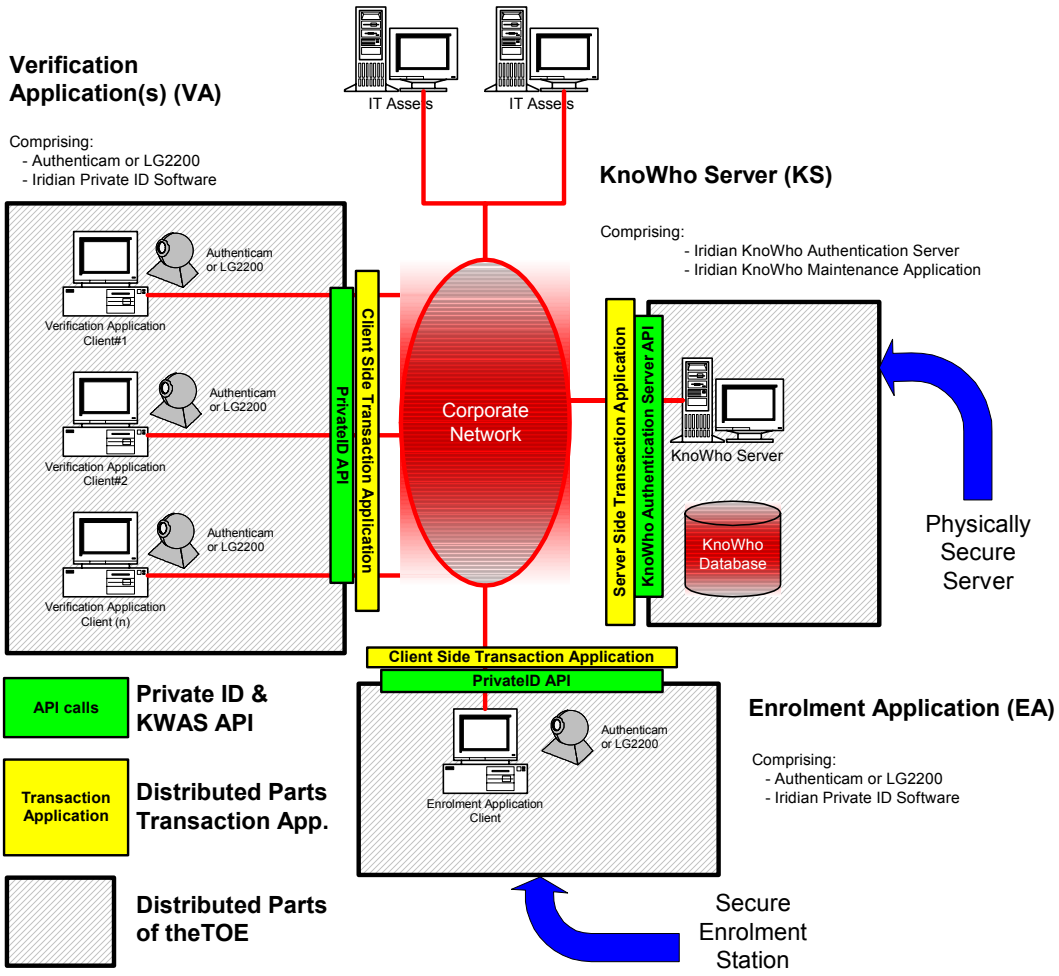
Once enrolled, an individual may be identified and/or verified for access to the IT resources protected by the TOE by providing a biometric sample using the camera. The sample is passed through to the KnoWho Authentication Server. Here the IrisCode is generated and compared with one or more stored biometric templates in the KnoWho Database. The Iridian KnoWho Server provides a response based on the success or failure of the comparisons, which is provided to the server-side of the transaction application, for further processing.

Organisations using the TOE will need to develop transaction applications appropriate to their requirements. These transaction applications will:

- Invoke TOE components (Private ID and KnoWho Authentication Server) using the appropriate API calls;
- Accept the API call responses received from the TOE components;
- Undertake any further processing required using the responses received from the TOE components; and
- Provide any additional security required for transmitting messages between separate elements of the transaction application, and from the transaction application to other organisational applications. For example, intra- and inter-application messages may be encrypted, signed, etc.

Figure 1 below shows a typical biometric application where TOE components have been grouped together to build Verification Application clients, an Enrolment Application client (Secure Enrolment Station) and a KnoWho Server component. Figure 1 also shows the use of transaction applications to request services from the TOE components, and to process the TOE responses. The transaction applications that interact with TOE components form part of a broader decision-making organisational application that will determine whether the corporate network will permit access to protected IT assets.

Figure 1: Example Application for KnoWho Server and Private ID



The TOE provides administrators with a GUI for effective security management of the biometric system through the Maintenance Application available only to administrators. The Maintenance Application enables administrators to set parameters for the enrolment, identification and verification of individuals, perform key and password management, and perform routine maintenance. For added security the TOE encrypts all stored biometric templates before being stored within the biometric database.

The TOE defines three distinct roles within its operational environment, these are:

- **TOE Administrators**, who are responsible for the secure management and operation of the TOE, including management of operator privilege;
- **TOE Operators**, who enrolment of users and maintenance of user enrolments; and
- **TOE Users**, who provide biometric samples to the TOE for identification, verification or enrolment.

2.2 Physical Scope of the TOE

The physical scope of the TOE includes the hardware and software elements identified in Table 1.

Table 1: Physical Components of the TOE

Physical TOE Components	Hardware/Software Platforms
Panasonic Authenticam Iris Recognition Camera manufactured by Panasonic, model BM-ET100US.	N/A
LG IrisAccess 2200 Iris Recognition Camera manufactured by LG, model 2200.	N/A
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; • 64 MB 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; • Windows NT4.0 workstation SP5 or later; or • Windows 2000 SP1 or later. Recommended Hardware Configuration: • Pentium 233MHz PC; • 64 MB RAM; • VGX FrameGrabber card; • Available serial port; • Network Interface Card; • Hard drive with sufficient capacity to store software; and • CD-ROM Drive for installation.

Physical TOE Components	Hardware/Software Platforms
Iridian KnoWho™ Authentication Server Iridian KnoWho Authentication Server Version 1.2.2 Iridian Maintenance Application	Operating Systems: • Windows NT4.0 Server Service Pack 5 or later; or • Windows 2000 Server or Advanced Server with Service Pack 1. RDBMS 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 400MHz; • 256Mb RAM; • RAID 5 configuration; • 9Gb Ultra-Wide SCSI HDD, average seek time 9ms, average latency 3ms; and • CD-ROM Drive for installation.

2.3 Security Features

A summary of the security features offered by the TOE is described in Table 2.

Table 2: Summary of TOE Security Features

Feature	Description
Biometric Identification of Individuals	Acceptance of biometric samples provided by individuals and generation IrisCodes for one-to-many (identification) comparison with stored biometric templates.
Biometric Verification of Individuals	Acceptance of biometric samples, with an identification number, provided by individuals and generation IrisCodes for one-to-one comparison with stored biometric templates.
Biometric Enrolment of Individuals	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 client PrivateID applications.
Forged Data Prevention	Prevention of the use of forged biometric data.
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.

2.4 Features Outside of Scope

Software and hardware features outside the scope of the defined TOE Security Functions (TSF) and thus not evaluated are:

- 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 the iris images, a user portrait image, the audit trail and configuration data for the TOE components.
- Encryption functionality other than 3DES used for confidentiality of the iris image during transmission, Message Authentication Code generation and database confidentiality;
- 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; and
- 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™ Server during installation of the TOE.

3 TOE Security Environment

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.
- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required.
- Any organisational security policy statements or rules with which the TOE must comply.

3.1 Secure Usage Assumptions

The following assumptions, listed in Table 3 below, relate to the operation of the TOE.

Table 3: Assumptions

Name	Description
A.ADMIN-DOCS	TOE Administrators will follow all policies and procedures described in the TOE system documentation to ensure secure administration of the TOE.
A.NO_EVIL	TOE Administrators and Operators are assumed to be non-hostile and trusted to perform all their duties in a competent manner.
A.KEYSOURCE	An appropriate source of cryptographic material, as defined by relevant National Authority Standards, to be used by the TOE must be available in the TOE environment.
A.ASSETS	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.
A.PHYS_SERVER	It is assumed that strong physical security measures will be in place to prevent unauthorised physical access to the server components of the TOE.
A.PHYS_ENROL	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.
A.PLATFORM	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.
A.NETWORK	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.

3.2 Threats to Security

Threats may be addressed either by the TOE or by its intended environment (for example, using personnel, physical, or administrative safeguards).

3.2.1 Threats Addressed by the TOE

The TOE addresses the following threats listed in Table 4 below.

Table 4:Threats Addressed by the TOE

Name	Description
T.CASUAL	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.
T.FAKE	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.
T.EVIL_TWIN	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.
T.REPLAY	An impostor uses a residual biometric image from a previous user to gain access to the IT assets protected by the TOE.
T.POORIMG	An impostor may direct an attack against a noisy or null image to gain access to the IT assets protected by the TOE.
T.BAD_ENROL	An unauthorised user attempts to illegally enrol on the biometric system in order to gain access to the IT assets protected by the TOE.
T.BAD_USER	A user attempts to exceed their privilege on the biometric system to gain unauthorised access to the IT assets protected by the TOE.
T.CORRUPT	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.
T.NO_DETECT	An attacker may attempt to mount a network-based attack against the TOE security functions, which succeeds without detection.
T.NOISE	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.

3.2.2 Threats Addressed by the Operating Environment

The TOE Operating Environment addresses the following threats listed in Table 5 below.

Table 5: Threats Addressed by the Operating Environment

Name	Description
TE.INSTALL	Those responsible for receiving and installing the TOE may unintentionally receive or install the TOE in a manner that undermines overall security.

3.3 Organisational Security Policies

Table 6 below describes the organisational security policies relevant to the operation of the TOE.

Table 6: Organisational Security Policies

Name	Description
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.
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 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 several roles.

4 Security Objectives

The security objectives are a concise statement of the intended response to the security problem. These objectives indicate, at a high level, how the security problem, as characterised in the "Security Environment" section of the ST, is to be addressed. Just as some threats are to be addressed by the TOE and others by its intended environment, so some security objectives are for the TOE and others are for its environment.

4.1 Security Objectives for the TOE

The security objectives for the TOE are as described in below in Table 7.

Table 7: Security Objectives for the TOE

Name	Description
O.FARFRR	The TOE shall provide the means to identify or verify individuals for access to IT assets, which is consistent with P.BIOMETRIC, and measured by the false acceptance rates (FAR) and false rejection rates (FRR) for the TOE.
O.ROLES	The TOE shall limit access to TOE security functions by individual on the basis of: • Their allocated role; and • The functions that are assigned to that role. in accordance with the organisational security policy P.ROLES.
O.NO_FORGE	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.
O.NO_FLOOD	The TOE shall resist optical-based physical attacks against the biometric capture device of the TOE.
O.AUDIT	The TOE shall record necessary events to ensure that all users of the TOE are held accountable for their actions.

4.2 Security Objectives for the Environment

The security objectives for the TOE environment are those specified in Table 8 below.

Table 8: Security Objectives for the Environment

Name	Description
OE.CRYPTO	Those responsible for the TOE shall ensure that procedures and/or mechanisms are in place to ensure that generation, storage and handling of cryptographic material is conducted in accordance with the rules defined by the organisational security policy P.CRYPTO.
OE.LOGICAL_ENV	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.
OE.PHYS_ENV	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.
OE.TRAIN	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.
OE.NETWORK	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.

5 IT Security Requirements

5.1 TOE Security Functional Requirements

This section contains the functional requirements for the TOE. The functional requirements are listed in Table 9, below.

Table 9: TOE Security Functional Requirements

No.	Component	Component Name
Class FAU: Audit		
1	FAU_GEN.1	Audit data generation
Class FCS: Cryptographic Support		
2	FCS_COP.1	Cryptographic operation
Class FIA: Identification and Authentication		
3	FIA_ATD.1	User attribute definition
4	FIA_UAU.2	User authentication before any action
5	FIA_UAU.3	Unforgeable authentication
6	FIA_UAU.5	Multiple authentication mechanisms
7	FIA_UAU.7	Protected authentication feedback
8	FIA_UID.2	User identification before any action
Class FMT: Security Management		
9	FMT_MOF.1	Management of security functions behaviour
10	FMT_MTD.1	Management of TSF Data
11	FMT_SMF.1	Specification of Management Functions
12	FMT_SMR.1	Security Roles
Class FPT: Protection of TSF Functions		
13	FPT_ITT.1	Basic internal TSF data transfer
14	FPT_ITT.3	TSF data integrity monitoring
15	FPT_PHP.3	Resistance to physical attack
16	FPT_RPL.1	Replay protection
17	FPT_STM.1	Reliable time stamps

The following sections contain the functional components from the Common Criteria Part 2 [CC2] (CC) with the operations completed.

5.1.1 Security audit (FAU)

Audit data generation (FAU_GEN.1)

Hierarchical to: No other components.

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

a) Start-up and shutdown of the audit functions; and

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

c) [success or failure of completed identification or verification attempt;

success or failure of completed enrolment or deletion attempt;

detection of modification of iris image data presented to the KnoWho Server; and

detected replay attacks].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, and [none].

Dependencies: FPT_STM.1 Reliable time stamps

5.1.2 Cryptographic support (FCS)

Cryptographic operation (FCS_COP.1)

Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform [data encryption and decryption, and calculation and verification of message authentication codes.] in accordance with a specified cryptographic algorithm [3DES] and cryptographic key sizes [168 bits], that meet the following: [requirements of Federal Information Processing Standard (FIPS) Publication 46-3, Data Encryption Standard, 25 October 1999].
Dependencies	[FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

5.1.3 Identification and Authentication (FIA)

User attribute definition (FIA_ATD.1)

Hierarchical to:	No other components
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [a) identifying name or number; b) unique physical characteristic; and c) role.]
Dependencies	No dependencies

User authentication before any action (FIA_UAU.2)

Hierarchical to:	FIA_UAU.1
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.
Dependencies	FIA_UID.1 Timing of identification

Unforgeable authentication (FIA_UAU.3)

Hierarchical to:	No other components.
FIA_UAU.3.1	The TSF shall *prevent* use of **biometric** authentication **request** data that has been forged **as a two-dimensional image** by any user of the TSF.
FIA_UAU.3.2	The TSF shall *prevent* use of **biometric** authentication **request** data that has been copied **as a two-dimensional image** from any other user of the TSF.
Dependencies	No dependencies.

Multiple authentication mechanisms (FIA_UAU.5)

Hierarchical to:	No other components.
FIA_UAU.5.1	The TSF shall provide [password, one-part physiological biometric and two-part physiological biometric authentication mechanisms] to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the [authentication SFP such that: a) if the user is requesting access to the KnoWho Server Maintenance Application then authenticate the user's claimed identity using the password mechanism before granting access to that application; b) if the user is requesting biometric identification for access to the IT assets under the control of the TOE, then authenticate the user's claimed identity using one-part physiological biometric authentication; c) if the user is requesting biometric verification for access to the IT assets under the control of the TOE, then authenticate the user's claimed identity using two-part physiological biometric authentication; d) if the user is a TOE Operator or a TOE Administrator supervising the enrolment of an individual then authenticate the TOE Operator or TOE Administrator supervising the enrolment using one-part physiological biometric authentication; or e) if the user is a TOE Operator or a TOE Administrator deleting the enrolment of an individual, then authenticate the TOE Operator or TOE Administrator requesting deletion of an enrolment using one-part physiological biometric authentication.]
Dependencies	No dependencies.

Protected authentication feedback (FIA_UAU.7)

Hierarchical to:	No other components.
FIA_UAU.7.1	The TSF shall provide only [feedback which indicates whether the identification or verification attempt was successful or unsuccessful] to the user while the **biometric** authentication is in progress.
Dependencies	FIA_UAU.1 Timing of authentication

User identification before any action (FIA_UID.2)

Hierarchical to:	FIA_UID.1
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.
Dependencies	No dependencies

5.1.4 Security Management (FMT)

Management of security functions behaviour (FMT_MOF.1 (1))

Hierarchical to:	No other components.
FMT_MOF.1.1(1)	The TSF shall restrict the ability to *determine the behaviour of, or modify the behaviour of* the functions [of the audit mechanism] to [TOE Administrators].
Dependencies	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security Roles

Management of security functions behaviour (FMT_MOF.1 (2))

Hierarchical to:	No other components.
FMT_MOF.1.1(2)	The TSF shall restrict the ability to *determine the behaviour of, enable, disable, and modify the behaviour of* the functions [to verify TOE Operators, to identify TOE Operators, to delete TOE Operators, and to enrol TOE Operators] to [TOE Administrators].
Dependencies	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security Roles

Management of security functions behaviour (FMT_MOF.1 (3))

Hierarchical to:	No other components.
FMT_MOF.1.1(3)	The TSF shall restrict the ability to *determine the behaviour of, enable, disable, and modify the behaviour of* the functions [to verify TOE Users, to identify TOE Users, to delete TOE Users, and to enrol TOE Users] to [TOE Administrators].
Dependencies	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security Roles

Management of security functions behaviour (FMT_MOF.1 (4))

Hierarchical to:	No other components.
FMT_MOF.1.1(4)	The TSF shall restrict the ability to *determine the behaviour of, enable, disable, and modify the behaviour of* the functions [for protecting the confidentiality and integrity of iris image data received by the KnoWho Server] to [TOE Administrators].
Dependencies	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security Roles

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

Hierarchical to:	No other components.
FMT_MTD.1.1(1)	The TSF shall restrict the ability to *delete and [initialise]* the [TOE User security attributes, i.e., identifying name or number, role and unique physical characteristic] to [TOE Administrators or TOE Operators].
Dependencies	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security Roles

Management of TSF data (FMT_MTD.1 (2))

Hierarchical to:	No other components.
FMT_MTD.1.1(2)	The TSF shall restrict the ability to *delete and [initialise]* the [TOE Operator security attributes, i.e., identifying name or number, role, and unique physical characteristic] to [TOE Administrators].
Dependencies	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security Roles

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

Hierarchical to:	No other components.
FMT_MTD.1.1(3)	The TSF shall restrict the ability to *query, modify, or delete* the [KnoWho Server configuration information] to [TOE Administrators].
Dependencies	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security Roles

Specification of Management Functions (FMT_SMF.1)

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: [management of the audit function, management of TOE User/Operator/Administrator identification/verification/enrolment functions and data, management of TOE roles and management of TOE configuration information].
Dependencies	No dependencies

Security roles (FMT_SMR.1)

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles: [TOE Users, TOE Operators, TOE Administrators].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies	FIA_UID.1 Timing of identification

5.1.5 Protection of TSF Functions (FPT)

Basic internal TSF data transfer protection (FPT_ITT.1)

Hierarchical to:	No other components.
FPT_ITT.1.1	The TSF shall protect TSF data from *disclosure and modification* when it is transmitted between separate parts of the TOE.
Dependencies	No dependencies

TSF data integrity monitoring (FPT_ITT.3)

Hierarchical to:	No other components.
FPT_ITT.3.1	The TSF shall be able to detect *modification of data* for TSF data transmitted between separate parts of the TOE.
FPT_ITT.3.2	Upon detection of a data integrity error, the TSF shall take the following actions: [audit the event].
Dependencies	FPT_ITT.1 Basic internal TSF data transfer protection

Resistance to physical attack (FPT_PHP.3)

Hierarchical to:	No other components.
FPT_PHP.3.1	The TSF shall resist [high-light level and low-light level optical based attacks] to the [biometric capture device] by responding automatically such that the TSP is not violated.
Dependencies	No dependencies

Replay detection (FPT_RPL.1)

Hierarchical to:	No other components.
FPT_RPL.1.1	The TSF shall detect replay for the following entities: [biometric data].
FPT_RPL.1.2	The TSF shall [reject the replayed data and audit the event] when replay is detected.
Dependencies	No dependencies

Reliable time stamps (FPT_STM.1)

Hierarchical to:	No other components.
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps for its own use.
Dependencies	No dependencies

5.2 TOE Security Assurance Requirements

This section contains the assurance requirements for the TOE. The assurance requirements are listed in Table 10, below.

Table 10: TOE Security Assurance Requirements

No.	Component	Component Name
Class ACM: Configuration management		
1	ACM_CAP.2	Configuration items
Class ADO: Delivery and Operation		
2	ADO_DEL.1	Delivery procedures
3	ADO_IGS.1	Installation, generation and start-up
Class ADV: Development		
4	ADV_FSP.1	Informal functional specification
5	ADV_HLD.1	Descriptive high level design
6	ADV_RCR.1	Informal representational correspondence
Class AGD: Guidance documents		
7	AGD_ADM.1	Administrator guidance
8	AGD_USR.1	User guidance
Class ATE: Tests		
9	ATE_COV.1	Evidence of coverage
10	ATE_FUN.1	Functional testing
11	ATE_IND.2	Independent testing- sample
Class AVA: Vulnerability Assessment		
12	AVA_SOF.1	Strength of TOE security function evaluation
13	AVA_VLA.1	Developer vulnerability analysis

5.2.1 Configuration management (ACM)

Configuration Items (ACM_CAP.2)

ACM_CAP.2.1D	The developer shall provide a reference for the TOE.
ACM_CAP.2.2D	The developer shall use a CM system.
ACM_CAP.2.3D	The developer shall provide CM documentation.
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.

5.2.2 Delivery and operation (ADO)

Delivery procedures (ADO_DEL.1)

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.
ADO_DEL.1.1C	The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

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

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

5.2.3 Development (ADV)

Informal functional specification (ADV_FSP.1)

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

Descriptive high-level design (ADV_HLD.1)

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

Informal correspondence demonstration (ADV_RCR.1)

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

5.2.4 Guidance documents (AGD)

Administrator guidance (AGD_ADM.1)

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

User guidance (AGD_USR.1)

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

5.2.5 Tests (ATE)

Evidence of coverage (ATE_COV.1)

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

Functional testing (ATE_FUN.1)

ATE_FUN.1.1D	The developer shall test the TSF and document the results.
ATE_FUN.1.2D	The developer shall provide test documentation.
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.

Independent testing - sample (ATE_IND.2)

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

5.2.6 Vulnerability Analysis (AVA)

Strength of TOE security functions (AVA_SOF.1)

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.
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.

Vulnerability analysis (AVA_VLA.1)

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.
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.

5.3 Security Requirements for the IT Environment

The TOE has the following requirements for the IT environment.

Cryptographic key generation (FCS_CKM.1)

Hierarchical to:	No other components
FCS_CKM.1.1	The **TOE environment** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [3DES] specified cryptographic key sizes [168 bit] that meets the following [requirements for cryptographic key generation, as defined by the Federal Information Processing Standard (FIPS) Publication 46-3, "Data Encryption Standard", 25 October 1999.]
Dependencies:	[FCS_CKM.2 Cryptographic key distribution **or** FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

5.4 Security Requirements for the Non-IT Environment

The TOE has the following security requirements for the Non-IT Environment.

ENV_NONIT.1 KnoWho Server is to be physically protected.

The KnoWho Server shall be located within a controlled access facility that will prevent unauthorised physical access.

ENV_NONIT.2 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.

ENV_NONIT.3 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.

ENV_NONIT.4 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 national authority standards.

ENV_NONIT.5 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.

ENV_NONIT.6 Configuration of infrastructure

The TOE environment shall provide procedures and guidance for the 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.

6 TOE Summary Specification

This section presents the Security Functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

6.1 Security Functions

Table 11 defines the IT security functions implemented by the TOE.

Table 11: IT Security Functions

IT Security Function Label	IT Security Function Description
IDENTIFY	The TOE provides services for the identification of TOE Users, TOE Operators and TOE Administrators. When the PrivateID software is invoked by a client-side transaction application, an individual presents their left or right iris to the camera on the client workstation, which takes a picture of the iris. The image is processed by the PrivateID software, which determines whether the supplied sample is of sufficient quality before being forwarded by the transaction application to the KnoWho server. The KnoWho Server generates an IrisCode from the sample that was captured by the PrivateID software, and compares the generated IrisCode against all enrolled IrisCodes stored within the biometric database. If the IrisCode matches an enrolled IrisCode, the KnoWho Server writes a recognition record to the audit trail and returns a response to the server-side of the transaction application, for further processing. If the IrisCode does not match any enrolled IrisCodes or an error has occurred, the KnoWho Server writes an error record to the audit trail with the reason why the identification failed and returns a response to the server-side of the transaction application, for further processing.

IT Security Function Label	IT Security Function Description
VERIFY	The TOE provides services for the verification of TOE Users, TOE Operators and TOE Administrators. When the PrivateID software is invoked by a client-side transaction application, an individual provides their identification number to the client-side of the transaction application and presents their left or right iris to the camera on the client workstation, which takes a picture of the iris. The image is processed by the PrivateID software, which determines whether the supplied sample is of sufficient quality before being forwarded, with the identification number, by the transaction application to the KnoWho server. The KnoWho Server generates an IrisCode from the sample that was captured by the PrivateID software, and compares the generated IrisCode with the enrolled IrisCode stored within the biometric database that is referenced by the identification number. If the IrisCode matches the enrolled IrisCode referenced by the identification number, the KnoWho Server writes a verification record to the audit trail and returns a response to the server-side of the transaction application. If the IrisCode does not match the enrolled IrisCode referenced by the identification number or an error has occurred, the KnoWho Server writes an error record to the audit trail with the reason why the verification failed and returns a response to the server-side of the transaction application.

IT Security Function Label	IT Security Function Description
ENROL_ADD	The TOE provides services for the enrolment of TOE Users, TOE Operators and TOE Administrators who may be enrolled with the left, right or both irises as required by the transaction application. For enrolment, the KnoWho Server requires four images of each of the individual's left, right or both irises, as appropriate, and an iris image for a TOE Operator with enrolment privilege (or in the case of TOE Operator enrolment, a TOE Administrator) authorising the enrolment. Each iris image must be captured by the PrivateID software and forwarded by the transaction application to the KnoWho Server. The PrivateID software processes the captured images in the same manner as the IDENTIFY and VERIFY functions. The TOE Administrator or TOE Operator supervising the enrolment process assigns the role for which the individual is to be enrolled. If the TOE Operator or TOE Administrator supervising then enrolment assigns a TOE Operator or TOE Administrator role for the individual, then a privilege level must also be provided to the KnoWho Server by the transaction application. The KnoWho Server then processes the received images by: • Selecting the highest quality image for each iris of those provided by the individual; • Identifying that a TOE Operator or TOE Administrator has authorised the enrolment; and • Confirming that the TOE Operator or TOE Administrator authorising the enrolment has enrolment privilege. Next, the KnoWho Server generates IrisCodes for the selected iris images and verifies that the left and right IrisCodes of the individual are unique with respect to one another, if both left and right iris images have been provided for the enrolment, and with all IrisCodes stored within the biometric database. If successful, the KnoWho Server generates an identification number for the individual, writes an enrolment record to the audit trail and the IrisCode into the biometric database, and sends a response to the server-side of the transaction application. The KnoWho Server writes an error record to the audit trail with the reason why the enrolment failed and sends a response to the server-side of the transaction application, if: • The iris images are of insufficient quality; or • The enrolees are already enrolled; or • The authorising operator has insufficient privilege to complete the operation.

IT Security Function Label	IT Security Function Description
ENROL_DEL	The TOE provides services for the deletion of TOE Administrator, TOE Operator and TOE User records. When the PrivateID software is invoked by a client-side transaction application, a TOE Operator or TOE Administrator provides the identification number of the enrolment record to be deleted to the client-side of the transaction application. They then present their left or right iris to the camera on the client workstation, which takes a picture of the iris. The image is processed by the PrivateID software, which determines whether the supplied sample is of sufficient quality before being forwarded by the transaction application, together with the identification number to the KnoWho server. The KnoWho Server then processes the data by: • Generating an IrisCode from the image and identifying that a TOE Operator or TOE Administrator has authorised the deletion of an enrolment record; and • Confirming that the TOE Operator or TOE Administrator authorising the deletion of the enrolment has delete enrolment privilege. Next, the KnoWho Server deletes the relevant record from the biometric database referenced by the identification number, writes a deletion record to the audit trail and sends a response to the server-side of the transaction application. If any step in the deletion process fails, the server writes an error record to the audit trail with the reason why the deletion failed and sends a response to the server-side of the transaction application.
TRANS_SEC	The KnoWho Server can detect replayed biometric data sent from a transaction application. The KnoWho Server accepts connection requests from transaction applications. In accepting the connection, the KnoWho Server generates a 16-byte nonce that is sent through the transaction application to the PrivateID software. The PrivateID software concatenates the nonce to the binary biometric image data, generates a CBC-MAC, and encrypts the image data before transmission to the KnoWho Server by the client-side of the transaction application. Upon receipt of the data, the KnoWho Server verifies that the decrypted data includes a valid nonce, and the CBC-MAC. If the nonce or the CBC-MAC is invalid, the KnoWho Server records the detail of the transaction in the appropriate audit trail and provides a response to the server-side of the transaction application. The KnoWho Server records all active nonces and can be configured by the TOE Administrator to store nonce values for a limited period of time. The nonces generated by the KnoWho Server may also be configured to time out after a TOE Administrator-configured period of time. The nonce timeout places a time-based restriction on the capture of iris images, thereby limiting the opportunity for the injection of forged biometric data The TOE provides for the confidentiality and integrity of all iris images captured by the PrivateID software and forwarded to the KnoWho Server by transaction applications.
BIO_DATA_CONF	The KnoWho Server provides confidentiality for stored biometric templates and binary biometric image data using 3DES encryption.

IT Security Function Label	IT Security Function Description
AUDIT	The KnoWho Server audits usage of the KnoWho Server security services by transaction applications for the following security-relevant events: • Success or failure of completed identification or verification attempts; • Success or failure of completed enrolment or deletion attempts; • Detection of authentication failure when two-dimensional fraudulent data is presented to the KnoWho Server during identification, verification, enrolment or deletion; • Detection of modification of iris image data presented to the KnoWho Server; and • Detected replay attacks. Some events related to incomplete transactions caused by misconfiguration of TOE components or lack of client response may not be captured in the audit trail, unless specifically entered by the server-side transaction application. The TOE maintains separate audit trails for TOE Operators and TOE Administrators, and TOE Users. The audit records may be configured to include or exclude binary data, however, at a minimum all audit records include: • Transaction ID; • Date/Time of the request; • Type of request; and • Result of the request (success or failure). Start-up and shutdown of the KnoWho Server service is also audited. The TOE uses its system time for time stamping audit entries.
SYS_MAN	The TOE provides a Maintenance Application to configure security parameters belonging to the KnoWho Server, the biometric database server, and the biometric database. To access the Maintenance Application, the TOE Administrator must enter the Administrator password. The Maintenance Application provides administrators with functionality to: • Set server parameters, such as: - listening port used by the KnoWho Server; - nonce generation and timeout parameters; - cryptographic keys and algorithms; • Enable or disable fraud detection; • Enable or disable server APIs for TOE User identification, verification and maintenance; • Enable or disable server APIs for TOE Operator identification, verification and maintenance; • Modify passwords used by the KnoWho Server, on behalf of the TOE Administrator; • Modify the audit function to include or exclude binary object data (iris images) in audit records.

6.2 Assurance Measures

The TOE claims to satisfy the assurance requirements for the Common Criteria Evaluation Assurance Level EAL2 (CC EAL2). Table 12 identifies the assurance measures relevant to the TOE that satisfy the CC EAL2 assurance requirements defined in the CC Part3 [CC3].

Table 12: Assurance Measures

Assurance Measure Label	Assurance Measure Description
CM_DOC	Configuration management documentation that includes a configuration list, a description of the configuration items comprising the TOE and a description of the method used to uniquely identify the configuration items. Document title(s): KnoWho Authentication Server and Private ID Configuration Management and Delivery Documentation, Version 1.2, August 2002
DEL_DOC	Delivery documentation that describes all procedures necessary to maintain security for distribution of the TOE to a user's site. Document title(s): KnoWho Authentication Server and Private ID Configuration Management and Delivery Documentation, Version 1. 2, August 2002
IGS_DOC	Installation and generation documentation that describes the steps necessary for secure installation, generation and start-up of the TOE. Document title(s): Iridian KnoWho Authentication Server Installation Guide, Document Number: 101875INS Revision-C, March 2002. Iridian Private ID™ with LG2200 Imager, Hardware and Software Installation Guide for Windows® 2000, Document Number: 102069INS, Revision-A, March 2002. Iridian Panasonic Authenticam™ Iris Recognition Camera Installation and Operation Guide for Windows® 2000 Operating System, Document Number: 101978UM Revision-A, September 2001. KnoWho Authentication Server and Private ID Installation and Administrator Guidance Addendum, Version 1.4, October 2002
FUN_SPEC	Functional specification that describes the TSF and its external interfaces and the purpose and method of use of external TSF interfaces, including details of effects, exceptions and error messages. Document title(s): KnoWho Authentication Server and Private ID Functional Specification, Version 1.5, August 2002
HLD_DOC	High-level design that describes the structure of the TSF in terms of sub-systems and describes the security functionality provided by each sub-system. Document title(s): KnoWho Authentication Server and Private ID High Level Design, Version 1.5, September 2002
RCR_DOC	Representation correspondence analysis that, for each adjacent pair TSF representations, demonstrates that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation. Document title(s): KnoWho Authentication Server and Private ID Representational Correspondence, Version 1.3, August 2002

Assurance Measure Label	Assurance Measure Description
ADMIN	Administrator guidance that describes the administrative functions and interfaces available to the administrator of the TOE, describes how to administer the TOE in a secure manner, describes warnings about functions and privileges that should be controlled in a secure processing environment, describes all assumptions about user behaviour relevant to secure operation, describes all security parameters under the control of the administrator, and describes 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. Document title(s): Iridian KnoWho™ Authentication Server Administrator's Manual, Document Number: 101934UM Revision-C, March 2002. KnoWho Authentication Server and Private ID Installation and Administrator Guidance Addendum, Version 1.4, October 2002
USER	User guidance that describes the functions and interfaces available to the non-administrative users of the TOE, describes the use of user accessible security functions, describes warnings about user accessible functions and privileges that should be controlled in a secure processing environment, and describes all user responsibilities necessary for secure operation of the TOE. Document title(s): Iridian Private ID™ with LG2200 Imager, Hardware and Software Installation Guide for Windows® 2000, Document Number: 102069INS Revision-A, March 2002. Iridian Panasonic Authenticam™ Iris Recognition Camera Installation and Operation Guide for Windows® 2000 Operating System, Document Number: 101978UM Revision-A, September 2001.
TEST_COV	Test evidence that shows the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification. Document title(s): KnoWho Authentication Server and Private ID Functional Testing and Coverage Analysis, Version 1.2, August 2002
TEST_DOC	The TOE and necessary supporting infrastructure suitable for testing. Test documentation consisting of test plans, test procedure descriptions, expected test results and actual test results. The test plan identifies the security functions to be tested and the goal of the tests to be performed. The test procedure descriptions identify the tests to be performed and describe the scenarios for testing each security function. The expected test results show the anticipated outputs from successful test execution. The actual test results demonstrate that each tested security function behaved as specified. Document title(s): KnoWho Authentication Server and Private ID Functional Testing and Coverage Analysis Version 1.2, August 2002
SOF_DOC	For each mechanism identified in the Security Target, an analysis shows that the claimed strength of TOE security function meets or exceeds the minimum strength level defined in the Security Target. Document title(s): KnoWho Authentication Server and Private ID Strength of Function Analysis, Version 1.1, August 2002

Assurance Measure Label	Assurance Measure Description
VLA_DOC	A vulnerability analysis that shows that for all identified vulnerabilities, the vulnerability cannot be exploited in the intended environment of the TOE. Document title(s): KnoWho Authentication Server and Private ID Vulnerability Analysis, Version 1.3, August 2002

7 PP Claims

The KnoWho Authentication Server and Private ID Security Target was not written to address a published Protection Profile.

8 Rationale

8.1 Security Objectives Rationale

The purpose of this rationale is to demonstrate that the identified security objectives are *suitable*, that is:

- They are *sufficient* to address the security needs; and
- They are *necessary*, i.e., there are no redundant security objectives.

8.1.1 All Assumptions, Policies and Threats Addressed

The need to demonstrate that there are no redundant security objectives is satisfied as follows:

- The first section (Table 13) shows that all of the secure usage assumptions, organisational security policies, and threats to security have been addressed.
- The second section (Table 14) shows that each security objective for the TOE and its environment counters at least one assumption, policy, or threat.

Table 13: Mapping of Threats, Assumptions and OSPs to Security Objectives

Label	Associated Security Objective
A.ADMIN-DOCS	OE.CRYPTO OE.TRAIN
A.NO_EVIL	O.ROLES O.AUDIT OE.TRAIN
A.KEYSOURCE	OE.CRYPTO
A.ASSETS	O.FARFRR
A.PHYS_SERVER	OE.PHYS_ENV
A.PHYS_ENROL	OE.PHYS_ENV
A.PLATFORM	OE.LOGICAL_ENV
A.NETWORK	OE.NETWORK
T.CASUAL	O.FARFRR O.AUDIT
T.FAKE	O.NO_FORGE O.AUDIT
T.EVIL_TWIN	O.FARFRR O.AUDIT
T.REPLAY	O.NO_FORGE O.AUDIT

Label	Associated Security Objective
T.POORIMG	O.FARFRR OE.TRAIN
T.BAD_ENROL	O.ROLES OE.TRAIN
T.BAD_USER	O.ROLES O.AUDIT OE.TRAIN
T.CORRUPT	O.ROLES O.AUDIT
T.NO_DETECT	O.AUDIT OE.TRAIN
T.NOISE	O.FARFRR O.NO_FLOOD
TE.INSTALL	OE.TRAIN
P.AUDIT	O.AUDIT OE.TRAIN
P.CRYPTO	OE.CRYPTO
P.TRAIN	OE.TRAIN
P.BIOMETRIC	O.FARFRR
P.ROLES	O.ROLES

Table 14 shows that there are no unnecessary IT security objectives.

Table 14: Mapping of Security Objectives to Threats, Policies and Assumptions

Objective Label	Threat / Policy/ Assumption
O.FARFRR	A.ASSETS T.CASUAL T.EVIL_TWIN T.POORIMG T.NOISE P.BIOMETRIC
O.ROLES	A.NO_EVIL T.BAD_ENROL T.BAD_USER T.CORRUPT P.ROLES
O.NO_FORGE	T.FAKE T.REPLAY
O.NO_FLOOD	T.NOISE
O.AUDIT	A.NO_EVIL T.CASUAL T.FAKE T.EVIL_TWIN T.REPLAY T.BAD_USER T.CORRUPT T.NO_DETECT P.AUDIT
OE.CRYPTO	A.ADMIN_DOCS A.KEYSOURCE P.CRYPTO
OE.LOGICAL_ENV	A.PLATFORM
OE.PHYS_ENV	A.PHYS_SERVER A.PHYS_ENROL

Objective Label	Threat / Policy/ Assumption
OE.TRAIN	A.ADMIN-DOCS A.NO_EVIL P.AUDIT T.BAD_ENROL T.BAD_IMAGE T.BAD_USER T.NO_DETECT TE.INSTALL P.TRAIN
OE.NETWORK	A.NETWORK

8.1.2 Security Objectives are Sufficient

The following arguments are provided in Table 15 to demonstrate the sufficiency of the Security Objectives outlined above.

Table 15: Sufficiency of Security Objectives

Label	Argument to support Security Objective sufficiency
A.ADMIN-DOCS	This assumption is upheld by the objectives OE.TRAIN and OE.CRYPTO as TOE Administrators and TOE Operators are required to receive appropriate training and documentation to enable them to operate and manage the TOE, and its associated cryptographic material, properly.
A.NO_EVIL	This assumption is upheld by the following security objectives: • O.ROLES provides for the limiting of access to TOE security functions based on defined roles; • O.AUDIT provides for the recording of security-relevant events and associating users with those events; and • OE.TRAIN ensures that TOE Administrators and TOE Operators receive appropriate training to enable them to operate the TOE securely. It also ensures that the organisation carries out the appropriate background checks and clearances for the individuals carrying out the TOE Administrator and TOE Operator roles.
A.KEYSOURCE	This assumption is upheld by the security objective OE.CRYPTO, which ensures that procedures and/or mechanisms exist in the TOE environment for the generation, storage and handling of cryptographic material.
A.ASSETS	This assumption is upheld by the security objective O.FARFRR, which ensures that the TOE meets national authority policy for use of biometric devices and a suitable FAR and FRR for identifying or verifying individuals prior to granting access to sensitive IT assets.
A.PHYS_SERVER	This assumption is upheld by OE.PHYS_ENV, which ensures that physical access to the TOE server components is appropriately controlled.

Label	Argument to support Security Objective sufficiency
A.PHYS_ENROL	This assumption is upheld by OE.PHYS_ENV, which ensures that physical access to the TOE enrolment components is appropriately controlled.
A.PLATFORM	This assumption is upheld by OE.LOGICAL_ENV, which ensures that logical access (including port connections) to the TOE server components is appropriately controlled.
A.NETWORK	This assumption is upheld by OE.NETWORK, which ensures that network connectivity between distributed parts of the TOE is provided via transaction applications.
T.CASUAL	The threat of a zero effort forgery is countered by the following security objectives: • O.FARFRR reduces the risk of an impostor making a successful zero effort forgery attempt as the FAR is appropriate for P.BIOMETRIC. This limits the chance of a successful attack. • O.AUDIT provides a deterrent to impostors making a zero effort forgery attempt by recording failed authentication attempts, thus increasing the likelihood that impostor will be detected.
T.FAKE	The threat of an impostor using a forged iris image of an authorised user is countered by the following security objectives: • O.NO_FORGE by ensuring that the TOE can prevent the use of two-dimensional forged biometric data; • O.AUDIT by ensuring that failed attempts to use forged biometric data are recorded, thus increasing the likelihood that an impostor will be detected.
T.EVIL_TWIN	The threat of an impostor us directing an attack against a similar biometric (e.g. samples taken from a twin) is countered by the following security objectives: • O.FARFRR which reduces the risk of an impostor making a successful attack against a similar (or twinned) biometric as the FAR is appropriate as required by P.BIOMETRIC for the intended biometric application. An appropriately low FAR correlates to a sufficient distinction between biometric samples such that the TOE will detect the differences between similar biometric samples. This limits the chance of a successful attack; and • O.AUDIT, which ensures that all attempts to be identified or verified by the TOE are recorded, thus increasing the likelihood that an impostor will be detected.
T.REPLAY	The threat of an impostor using a residual biometric image from a previous user is countered by the following security objectives: • O.NO_FORGE, which ensures that the TOE can detect and prevent the use of forged biometric data (including replayed information); and • O.AUDIT, which ensures that attempts to be identified or verified by the TOE are recorded, thus increasing the likelihood that a replay attack will be detected.

Label	Argument to support Security Objective sufficiency
T.POORIMG	The threat of an attack directed against a noisy or null image is countered by the following security objectives: • O.FARFRR ensures that the TOE complies with the appropriate National Authority policy for use of biometric devices as measured by its FAR. A TOE that meets the O.FARFRR objective is less likely to accept a noisy or dull image when comparing against enrolled biometric templates. • OE.TRAIN ensures that TOE Administrators and TOE Operators receive appropriate training to enable them to operate the TOE securely. This training includes processes for secure enrolment of authorised users.
T.BAD_ENROL	The threat of illegal enrolment of an impostor is countered by the following security objectives: • O.ROLES ensures that access to the enrolment functions are restricted to only authorised TOE Administrators and TOE Operators; and • OE.TRAIN reduces the risk of security procedural errors that might lead to an illegal enrolment, by ensuring that appropriately trained personnel supervise all enrolments.
T.BAD_USER	The threat of a user attempting to exceed their authority is countered by the following security objectives: • O.ROLES prevents users from performing actions on the IT Security Functions outside that which is defined by their designated role. • O.AUDIT provides the capability to record security relevant events that might indicate an attempt by a user to exceed their authority. • OE.TRAIN reduces the risk that users will attempt to exceed their authority by providing users with security awareness training.
T.CORRUPT	The threat of unauthorised modification of security-relevant data is countered by the following security objectives: • O.ROLES restricts the ability to modify the security-relevant data such as the audit trail and configuration parameters to specific roles. • O.AUDIT, which ensures that security-relevant events for the TOE are recorded, thus increasing the likelihood that a modification of the TOE configuration will be detected.
T.NO_DETECT	The threat of an undetected attack is countered by the following security objectives: • O.AUDIT, which ensures that all security-relevant events that may indicate an attack on the TOE security functions are recorded and that information recorded is sufficient to hold individual users accountable for their security-relevant actions. • OE.TRAIN, which ensures that TOE Administrators and TOE Operators receive appropriate training for the secure management and operation of the TOE. This training includes procedures for the regular inspection and review of the audit trails, and awareness training to detect possible attacks on the TOE.

Label	Argument to support Security Objective sufficiency
T.NOISE	The threat of optical-based flooding attacks is countered by the following security objectives: • O.FARFRR, which ensures that the TOE complies with the appropriate National Authority policy in use of biometric devices as measured by its FAR. A TOE that meets the O.FARFRR objective is less likely to accept a noisy or dull image when comparing against enrolled biometric templates. • O.NO_FLOOD, which ensures that the TOE resists attempts to optically flood the biometric capture device to provide a noisy or dull image for comparison against enrolled
TE.INSTALL	The threat that the TOE may be delivered and installed in a manner that undermines security is countered by the security objective OE.TRAIN, which requires that all individuals (TOE Administrators, TOE Operators and TOE Users) receive appropriate training in the management and operation of the TOE according to their role.
P.AUDIT	The OSP requirement for appropriate archive of audit records is met by the following security objectives: • O.AUDIT provides functionality to record security-relevant events in such a way that an individual may be held accountable for their security-relevant actions. • OE.TRAIN ensures that appropriate training is provided to TOE Administrators and TOE Operators for the secure operation and management of the TOE, which includes archive of audit records in accordance with an organisation's archive requirements.
P.CRYPTO	The OSP requirement for appropriate management of cryptographic key material is met by OE.CRYPTO, which requires an organisation to manage its cryptographic material in accordance with the relevant National Authority Standards for the protection of such material. E.g. For Commonwealth Government Agencies, the appropriate National Authority Standard is the Australian Communications-Electronic Security Instruction (ACSI) 57.
P.TRAIN	The OSP requirement that individuals receive appropriate security awareness training is met by the OE.TRAIN security objective, which ensures that all individuals (TOE Administrators, TOE Operators and TOE Users) receive appropriate training for the TOE.
P.BIOMETRIC	The OSP requirement that National Authority policy must be satisfied in respect of the use of biometric devices, is met by the security objective O.FARFRR, which requires that the TOE meets National Authority policy and is measured by its FAR and FRR.
P.ROLES	The OSP requirement for assigning individuals to roles is met by O.ROLES, which requires access to TOE security functions is restricted on the basis of defined roles.

8.2 Security Requirements Rationale

8.2.1 Suitability of the Security Requirements

The purpose of this section is to show that the identified security requirements are *suitable* to meet the security objectives. Table 16 and Table 17 show that each security requirement is *necessary,* that is, each security objective is addressed by at least one security requirement and vice versa. Note that several objectives are partially satisfied by the TOE and partially satisfied by the IT environment.

Table 16: Mapping of Security Objectives to Security Requirements

Objectives	Requirements
O.FARFRR	FIA_ATD.1, FIA_UAU.2, FIA_UAU.5, FIA_UAU.7, FIA_UID.2
O.ROLES	FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FIA_UAU.5, FMT_MOF.1(1), FMT_MOF.1(2), FMT_MOF.1(3), FMT_MOF.1(4), FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_SMF.1, FMT_SMR.1
O.NO_FORGE	FCS_COP.1, FIA_UAU.3, FPT_ITT.1, FPT_ITT.3, FPT_RPL.1
O.NO_FLOOD	FPT_PHP.3
O.AUDIT	FAU_GEN.1, FIA_UID.2, FIA_UAU.2, FMT_MOF.1(1), FPT_STM.1
OE.CRYPTO	FCS_CKM.1 ENV_NONIT.4
OE.LOGICAL_ENV	ENV_NONIT.5, ENV_NONIT.6
OE.PHYS_ENV	ENV_NONIT.1, ENV_NONIT.2
OE.TRAIN	ENV_NONIT.3
OE.NETWORK	ENV_NONIT.6

Table 17: Mapping of Security Requirements to Security Objectives

Requirements	Objective
FAU_GEN.1	O.AUDIT
FCS_COP.1	O.NO_FORGE
FIA_ATD.1	O.FARFRR O.ROLES
FIA_UAU.2	O.FARFRR O.ROLES O.AUDIT

Requirements	Objective
FIA_UAU.3	O.NO_FORGE
FIA_UAU.5	O.FARFRR O.ROLES
FIA_UAU.7	O.FARFRR
FIA_UID.2	O.FARFRR O.ROLES O.AUDIT
FMT_MOF.1(1)	O.ROLES O.AUDIT
FMT_MOF.1(2)	O.ROLES
FMT_MOF.1(3)	O.ROLES O.AUDIT
FMT_MOF.1(4)	O.ROLES
FMT_MTD.1(1)	O.ROLES
FMT_MTD.1(2)	O.ROLES
FMT_MTD.1(3)	O.ROLES
FMT_SMF.1	O.ROLES
FMT_SMR.1	O.ROLES
FPT_ITT.1	O.NO_FORGE
FPT_ITT.3	O.NO_FORGE
FPT_PHP.3	O.NO_FLOOD
FPT_RPL.1	O.NO_FORGE
FPT_STM.1	O.AUDIT
FCS_CKM.1	OE.CRYPTO
ENV_NONIT.1	OE.PHYS_ENV
ENV_NONIT.2	OE.PHYS_ENV
ENV_NONIT.3	OE.TRAIN
ENV_NONIT.4	OE.CRYPTO
ENV_NONIT.5	OE.LOGICAL_ENV
ENV_NONIT.6	OE.LOGICAL_ENV OE.NETWORK

8.2.2 Sufficiency of the Security Requirements

The following table shows that security requirements are *sufficient* to satisfy the TOE security objectives, whether in a principal or supporting role.

Table 18: Sufficiency of Security Requirements

Objectives	Argument to support sufficiency of Security Requirements
O.FARFRR	The objective to meet the National Authority Standards for the FAR and FRR is met by the following security requirements: • FIA_UID.2 and FIA_UAU.2 provide support to the achievement of mandated FAR and FRR by requiring identification and authentication of the users such that access to the IT resources protected by the TOE is permitted to authorised users and denied to all other individuals. • FIA_UAU.5 provide support to FIA_UID.2 and FIA_UAU.2 by ensuring the appropriate authentication mechanism to meet FAR FRR during biometric identification or verification. • FIA_UAU.7 ensures that no feedback is provided to an impostor that could be exploited in subsequent attacks to defeat the biometric authentication mechanism. • FIA_ATD.1 provides support to the TOE security policy enforcement by requiring that relevant user security attributes be recognised by the TOE and associated with users, including the identifying name or number, and unique physical characteristics. • AVA_SOF.1 ensures that the objective is met since it requires validation that the explicit strength metric, indicated by the required FAR and FRR values, is met by the TOE.

Objectives	Argument to support sufficiency of Security Requirements
O.ROLES	The objective to limit access to the TOE security functions based on defined roles is met by the following security requirements: • FIA_ATD.1 associates a user role with their user identity. • FIA_UID.2 and FIA_UAU.2 provide support to meet this objective by requiring identification and authentication of all users (TOE Administrators, TOE Operators and TOE Users). • FIA_UAU.5 supports FIA_UID.2 and FIA_UAU.2 by ensuring that the appropriate authentication mechanism is applied for the point of access to the TOE Security Functions (e.g. at the server or through a secure enrolment station). • FMT_SMR.1 requires that the TOE be able to recognise the roles and to be able to associate users with their roles. • FMT_SMF.1 requires that the TOE provides functions for security management of the TOE. • FMT_MOF.1(1) requires that the ability to tune the performance of the audit mechanism be restricted to TOE Administrators. • FMT_MOF.1(2) requires that the ability to manage TOE Operator enrolment, identification and verification functions is restricted to TOE Administrators. • FMT_MOF.1(3) requires that the ability to manage TOE User enrolment, identification and verification functions is restricted to TOE Administrators. • FMT_MOF.1(4) requires that the ability to manage KnoWho Server generated nonces that provide for integrity iris image data is restricted to TOE Administrators. • FMT_MTD.1 (1) requires that the ability to manage TOE User security attributes is restricted to TOE Administrators and TOE Operators. • FMT_MTD.1(2) requires that the ability to manage TOE Operator security attributes is restricted to TOE Administrators. • FMT_MTD.1(3) requires that the ability to manage TOE configuration information is restricted to TOE Administrators.

Objectives	Argument to support sufficiency of Security Requirements
O.NO_FORGE	The objective to detect and prevent forgery of authentication data is met by the following security requirements: • As refined within this Security Target, FIA_UAU.3 requires that the TOE must prevent forgeries using two-dimensional image data. Further, FIA_UAU.3 requires the TOE to prevent an individual from using the biometric reference template of another user. • FPT_ITT.1 protects TSF data from disclosure and modification when it is transmitted between separate parts of the TOE, e.g. between the verification application and the TOE server components. • FPT_ITT.3 requires the TOE to detect attempts to compromise the integrity of TSF data when it is transmitted between separate parts of the TOE, thereby helping to prevent attempted forgery attacks. • FPT_RPL.1 requires the TOE to block attacks based on the capture and replay of biometric authentication data. • FCS_COP.1, supports FPT_ITT.1 in meeting the security objective by requiring the TOE to provide cryptographic operations for the protecting the confidentiality and integrity of information transmitted between separate parts of the TOE. • FCS_COP.1 also protects binary data (IrisCodes and iris images) stored in the biometric database by encrypting the data using 3DES, limiting the opportunity for an attacker to gain access to IrisCodes or iris images to mount forgery attacks.
O.NO_FLOOD	The objective to resist optical-based physical attacks against the biometric capture device of the TOE is met by the security requirement FPT_PHP.3, which requires the TOE to resist high-light and low-light level optical based attacks to the biometric capture device.
O.AUDIT	The objective to provide the means of detecting and recording security relevant events is met by the following security requirements: • FAU_GEN.1 requires the capability to generate records of security relevant events, including the identity of the user responsible in order to be able to hold a user accountable for their actions. • FIA_UAU.2 and FIA_UID.2 together support FAU_GEN.1 by requiring the TOE to enforce identification and authentication of all users. • FPT_STM.1 requires the provision of reliable time stamps that can be associated with security-relevant events. • FMT_MOF.1 (1) require that the ability to manage the audit functions be restricted to administrators. This security requirements help to ensure that appropriate audit data is collected and maintained by the TOE.
OE.CRYPTO	This objective is met by the following security requirements: • FCS_CKM.1 requires that an appropriate key generation mechanism, for all confidentiality keys used by the TOE, is available within the environment. • ENV_NONIT.4 requires that cryptographic material is appropriately stored and handled in accordance with national authority standards defined in P.CRYPTO.

Objectives	Argument to support sufficiency of Security Requirements
OE.LOGICAL_ENV	This objective is met by the following security requirements: • ENV_NONIT.5 requires that the ports available for TCP/IP connection for the TOE server components are restricted to only those used by the TOE. • ENV_NONIT.6 requires that the underlying operating systems controls for identification and authentication are properly configured such that no other user accounts on the underlying operating system exist.
OE.PHYS_ENV	This objective is met by the following security requirements: • ENV_NONIT.1 requires that the KnoWho server component is located in a controlled access facility, reducing the likelihood that an attacker could compromise the security of the TOE by gaining physical access. • ENV_NONIT.2 requires that the secure enrolment stations are located in a controlled access facility, reducing the likelihood of an illegal enrolment the could allow an attacker to gain access to the IT assets protected by the TOE.
OE.TRAIN	This objective is met by the following security requirements: • ENV_NONIT.3 requires that all personnel using, operating or administering the TOE are appropriately trained according to their role.
OE.NETWORK	This objective is met by the following security requirements: • ENV_NONIT.6 requires that appropriate network connectivity is provided between distributed parts of the TOE via transaction applications.

8.2.3 Satisfaction of Dependencies

Table 19 shows the dependencies between the functional requirements. All of the dependencies are satisfied. Note that:

(H) indicates the dependency is satisfied through the inclusion of a component that is hierarchical to the one required).

(*) indicates that the TOE does not satisfy this dependency. Refer to the supporting rationale following Table 19.

Table 19: Dependency Analysis

Component Reference	Requirement	Dependencies	Dependency Reference
Functional Requirements			
1	FAU_GEN.1	FPT_STM.1	17
2	FCS_COP.1	FCS_CKM.1*, FCS_CKM.4*, FMT_MSA.2*	-
3	FIA_ATD.1	No dependencies	-
4	FIA_UAU.2	FIA_UID.1	8(H)
5	FIA_UAU.3	No dependencies	-
6	FIA_UAU.5	No dependencies	-
7	FIA_UAU.7	FIA_UAU.1	4(H)
8	FIA_UID.2	No dependencies	-
9	FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	11, 12
10	FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	11, 12
11	FMT_SMF.1	No dependencies	-
12	FMT_SMR.1	FIA_UID.1	8(H)
13	FPT_ITT.1	No dependencies	-
14	FPT_ITT.3	FPT_ITT.1	13
15	FPT_PHP.3	No dependencies	-
16	FPT_RPL.1	No dependencies	-
17	FPT_STM.1	No dependencies	-
Assurance Requirements			
18	ACM_CAP.2	None	-
19	ADO_DEL.1	None	-
20	ADO_IGS.1	AGD_ADM.1	24
21	ADV_FSP.1	ADV_RCR.1	23
22	ADV_HLD.1	ADV_FSP.1, ADV_RCR.1	21, 23

Component Reference	Requirement	Dependencies	Dependency Reference
23	ADV_RCR.1	None	-
24	AGD_ADM.1	ADV_FSP.1	21
25	AGD_USR.1	ADV_FSP.1	21
26	ATE_COV.1	ADV_FSP.1, ATE_FUN.1	21, 27
27	ATE_FUN.1	None	-
28	ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1	21, 24, 25, 27
29	AVA_SOF.1	ADV_FSP.1, ADV_HLD.1	21, 22
30	AVA_VLA.1	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1	21, 22, 24, 25

The following dependencies are not satisfied in this Security Target:

- FMT_MSA.2 Secure security attributes;
- FCS_CKM.1 Cryptographic key generation; and
- FCS_CKM.4 Cryptographic key destruction.

FMT_MSA.2 is identified as a dependency for FCS_COP.1. The intent of FMT_MSA.2 is that values for security attributes must not violate the TSP. In the context of the FCS family, FMT_MSA.2 requires that the combination of cryptographic security attributes such as key length, key validity period and key use (e.g. digital signature, key encryption, data encryption) may only be set to values which maintain the 'secure state' of the TOE. Cryptographic functionality of the TOE is subject to independent evaluation by the National Authority for cryptography, which includes evaluation of the combination of cryptographic security attributes that will maintain the 'secure state'. This Security Target, and the guidance documentation clearly identify the combination of cryptographic attributes that are required to maintain a secure state; therefore, the requirement FCS_COP.1 is met without satisfying this dependency.

FCS_CKM.1 is identified as a dependency for FCS_COP.1. The TOE provides no functionality for the generation of cryptographic keys. Instead, an appropriately trusted source of keys must be provided in the TOE environment. This has been reflected in the security requirement for the IT environment FCS_CKM.1. Therefore, the requirement FCS_COP.1 is met without satisfying this dependency.

FCS_CKM.4 is identified as a dependency for FCS_COP.1. The TOE provides no functionality for the destruction of cryptographic keys. Instead, all cryptographic material used for the implementation of FCS_COP.1 is held until overwritten by new cryptographic material generated in the TOE environment as required by FCS_CKM.1. All cryptographic material must be stored and handled in accordance with

national authority standards. This has been reflected in the security requirement for the non-IT environment ENV_NONIT.4. Therefore, the requirement FCS_COP.1 is met without satisfying this dependency.

8.3 TOE Summary Specification Rationale

8.3.1 IT security functions satisfy the SFRs.

The following two tables show that each SFR is mapped to at least one IT security function and each IT security function is mapped to at least one SFR.

Table 20: Mapping of SFRs to IT Security Functions

Security Functional Requirement	IT Security Function
FAU_GEN.1	AUDIT
FCS_COP.1	BIO_DATA_CONF TRANS_SEC
FIA_ATD.1	ENROL_ADD
FIA_UAU.2	IDENTIFY VERIFY ENROL_ADD ENROL_DEL SYS_MAN
FIA_UAU.3	IDENTIFY VERIFY ENROL_ADD ENROL_DEL TRANS_SEC
FIA_UAU.5	IDENTIFY VERIFY ENROL_ADD ENROL_DEL SYS_MAN
FIA_UAU.7	IDENTIFY VERIFY ENROL_ADD ENROL_DEL

Security Functional Requirement	IT Security Function
FIA_UID.2	IDENTIFY VERIFY ENROL_ADD ENROL_DEL SYS_MAN
FMT_MOF .1(1)	SYS_MAN
FMT_MOF.1(2)	SYS_MAN
FMT_MOF.1(3)	SYS_MAN
FMT_MOF.1(4)	SYS_MAN
FMT_MTD.1(1)	ENROL_ADD ENROL_DEL
FMT_MTD.1(2)	ENROL_ADD ENROL_DEL
FMT_MTD.1(3)	SYS_MAN
FMT_SMF.1	ENROL_ADD ENROL_DEL SYS_MAN
FMT_SMR.1	ENROL_ADD
FPT_ITT.1	TRANS_SEC
FPT_ITT.3	TRANS_SEC
FPT_PHP.3	IDENTIFY VERIFY ENROL_ADD ENROL_DEL
FPT_RPL.1	TRANS_SEC
FPT_STM.1	AUDIT

Table 21: Mapping of IT Security Functions to SFRs

IT Security Function	Security Functional Requirement
IDENTIFY	FIA_UAU.2 FIA_UAU.3 FIA_UAU.5 FIA_UAU.7 FIA_UID.2 FPT_PHP.3
VERIFY	FIA_UAU.2 FIA_UAU.3 FIA_UAU.5 FIA_UAU.7 FIA_UID.2 FPT_PHP.3
ENROL_ADD	FIA_ATD.1 FIA_UAU.2 FIA_UAU.3 FIA_UAU.5 FIA_UAU.7 FIA_UID.2 FMT_MTD.1(1) FMT_MTD.1(2) FMT_SMF.1 FMT_SMR.1 FPT_PHP.3
ENROL_DEL	FIA_UAU.2 FIA_UAU.3 FIA_UAU.5 FIA_UAU.7 FIA_UID.2 FMT_MTD.1(1) FMT_MTD.1(2) FMT_SMF.1 FPT_PHP.3

IT Security Function	Security Functional Requirement
TRANS_SEC	FCS_COP.1 FIA_UAU.3 FPT_ITT.1 FPT_ITT.3 FPT_RPL.1
BIO_DATA_CONF	FCS_COP.1
AUDIT	FAU_GEN.1 FPT_STM.1
SYS_MAN	FIA_UAU.2 FIA_UAU.5 FIA_UID.2 FMT_MOF.1(1) FMT_MOF.1(2) FMT_MOF.1(3) FMT_MOF.1(4) FMT_MTD.1(3) FMT_SMF.1

8.3.2 IT Security Function Suitability

Table 22 provides appropriate justification that the IT Security Functions are suitable to meet the TOE Security Functional Requirement and that when implemented, contributes to meeting that requirement.

Table 22: Suitability of IT Security Functions

Security Functional Requirement	Argument for suitability of IT Security Functions
FAU_GEN.1	The TOE SFR is satisfied by the IT Security Function AUDIT as: • the function provides for the generation of audit records that are written to an audit trail. The AUDIT function is started automatically when the KnoWho Server service is started and operates continuously until the KnoWho Server service is stopped. Given that KnoWho Server service start and stop are audited, the start-up and shutdown of the audit functions are, by default, audited.
FCS_COP.1	The TOE SFR is satisfied by the IT Security Functions BIO_DATA_CONF and TRANS_SEC as: • BIO_DATA_CONF provides 3DES encryption services for confidentiality of binary data (IrisCodes and iris images) stored in the biometric database and audit trail. • TRANS_SEC provides 3DES encryption services for the encryption of iris image data and the generation of a message authentication code (MAC) when transmitting biometric samples to the KnoWho server for identification, verification or enrolment.
FIA_ATD.1	The TOE SFR is satisfied by the IT Security Function ENROL_ADD as: • this function requires the provision of a biometric sample, the definition of role during the enrolment process, to which a unique identification number is assigned by the KnoWho server for that enrolment record.
FIA_UAU.2	The TOE SFR is satisfied by the IT Security Functions IDENTIFY, VERIFY, ENROL_ADD, ENROL_DEL and SYS_MAN as: • IDENTIFY, VERIFY, ENROL_ADD and ENROL_DEL provide for the authentication of a TOE User, TOE Operator or TOE Administrator against a stored biometric template before an individual may take any actions through the TOE. • SYS_MAN ensures that TOE Administrators are authenticated by supplying the administrative password to the maintenance application before they can take any actions through the TOE.

Security Functional Requirement	Argument for suitability of IT Security Functions
FIA_UAU.3	The TOE SFR is satisfied by the IT Security Functions IDENTIFY, VERIFY, ENROL_ADD, ENROL_DEL and TRANS_SEC as: • IDENTIFY, and VERIFY provide the capability to prevent the use of two-dimensional forged data. • ENROL_ADD and ENROL_DEL provide the capability to prevent the use of two-dimensional forged data in the authentication of the TOE administrator authorising the enrolment or deletion. • TRANS_SEC restricts the opportunity for an attacker to use forged biometric data to gain access to the IT resources protected by the TOE, by limiting the time available for the acquisition of biometric images. • TRANS_SEC restricts the opportunity for an attacker to gain access to the IT resources protected by the TOE, by copying and replaying session data captured in transit between components of the TOE, back to the KnoWho Server.
FIA_UAU.5	The TOE SFR is satisfied by the IT Security Functions IDENTIFY, VERIFY, ENROL_ADD, ENROL_DEL and SYS_MAN as: • these functions all provide for the authentication of TOE Users, TOE Operators and TOE Administrators using different authentication mechanisms as specified by the authentication SFP.
FIA_UAU.7	The TOE SFR is satisfied by the IT Security Functions IDENTIFY, VERIFY, ENROL_ADD and ENROL_DEL as: • these functions limit the information returned to the verification or enrolment client on the current verification or identification attempt.
FIA_UID.2	The TOE SFR is satisfied by the IT Security Functions IDENTIFY, VERIFY, ENROL_ADD, ENROL_DEL and SYS_MAN as: • IDENTIFY and VERIFY ensure that a TOE User, TOE Operator or TOE Administrator is uniquely identified by the TOE before any other action. • ENROL_ADD and ENROL_DEL ensure that a TOE Operator with appropriate privilege or a TOE Administrator is uniquely identified before accepting or deleting an enrolment. • SYS_MAN ensures that TOE Administrators are identified before allowing access to the maintenance application of the TOE.
FMT_MOF.1(1)	The TOE SFR is satisfied by the IT Security Function SYS_MAN as: • the function restricts the ability to modify the behaviour of the audit mechanism to only authorised TOE Administrators through the maintenance application.
FMT_MOF.1(2)	The TOE SFR is satisfied by the IT Security Function SYS_MAN as: • the function restricts the ability to enable or disable APIs for TOE Operator identification, verification and maintenance to only authorised TOE Administrators through the maintenance application.
FMT_MOF.1(3)	The TOE SFR is satisfied by the IT Security Function SYS_MAN as: • the function restricts the ability to enable or disable APIs for TOE User identification, verification and maintenance to only authorised TOE Administrators through the maintenance application.

Security Functional Requirement	Argument for suitability of IT Security Functions
FMT_MOF.1(4)	The TOE SFR is satisfied by the IT Security Function SYS_MAN as: the function restricts the ability to configure the generation of KnoWho Server nonces and the selection of acceptable cryptographic algorithms to only authorised TOE Administrators through the maintenance application.
FMT_MTD.1(1)	The TOE SFR is satisfied by the IT Security Functions ENROL_ADD and ENROL_DEL as: • ENROL_ADD and ENROL_DEL restrict the ability to initialise and delete TOE User security attributes to authorised TOE Administrators and TOE Operators during enrolment.
FMT_MTD.1(2)	The TOE SFR is satisfied by the IT Security Functions ENROL_ADD and ENROL_DEL as: • ENROL_ADD and ENROL_DEL restrict the ability to initialise, clear and delete TOE Operator security attributes to authorised TOE Administrators during enrolment.
FMT_MTD.1(3)	The TOE SFR is satisfied by the IT Security Functions SYS_MAN as: • SYS_MAN restricts the ability to query or modify or delete security attributes associated with the generation, archiving and timeout period for KnoWho Server nonces to authorised TOE Administrators through the maintenance application.
FMT_SMF.1	The TOE SFR is satisfied by the IT Security Functions ENROL_ADD, ENROL_DEL and SYS_MAN as: • ENROL_ADD and ENROL_DEL provide the means for TOE Operators or TOE Administrators to enrol TOE Users, TOE Operators or TOE Administrators and delete enrolment records held by the TOE. • SYS_MAN provides the means for TOE Administrators to manage the TOE Security Functions through the maintenance application.
FMT_SMR.1	The TOE SFR is satisfied by the IT Security Function ENROL_ADD as: • ENROL_ADD provides for the maintenance and assignment of individual roles through enrolment of TOE Administrators, TOE Operators and TOE Users.
FPT_ITT.1	The TOE SFR is satisfied by the IT Security Function TRANS_SEC as: • this function ensures the confidentiality and integrity of data transmitted between the enrolment and verification applications and the KnoWho Server through implementation of message authentication codes (MACs).
FPT_ITT.3	The TOE SFR is satisfied by the IT Security Function TRANS_SEC as: • this function detects modification of data transmitted between the enrolment and verification applications and the KnoWho Server through implementation of message authentication codes (MACs).
FPT_PHP.3	The TOE SFR is satisfied by the IT Security Functions IDENTIFY, VERIFY, ENROL_ADD and ENROL_DEL as: • IDENTIFY, VERIFY, ENROL_ADD and ENROL_DEL all provide functionality that reject biometric samples from the capture device that are of insufficient quality, as might result from optical-based attacks on the capture device.

Security Functional Requirement	Argument for suitability of IT Security Functions
FPT_RPL.1	The TOE SFR is satisfied by the IT Security Function TRANS_SEC as: • this function provides the means for the detection of replayed authentication data from a verification or enrolment client to the KnoWho Server with an associated audit record being generated and stored within the biometric database.
FPT_STM.1	The TOE SFR is satisfied by the IT Security Function AUDIT as: • this function generates and associates timestamps with each security-relevant event written to the audit trail. AUDIT uses the KnoWho server system time as the clock source.

8.3.3 Demonstration of Mutual Support

The primary function of the TOE, namely identification or verification of users, is provided by the SFRs from the FIA class. The SFRs selected from the FAU class provide the auditing functions in support of the FIA requirements by recording security-relevant events that might indicate a potential compromise of those functions. These are in turn supported by the SFRs from the FMT, FCS and FPT classes as follows:

- SFRs from the FMT class provide TOE Administrator and TOE Operator functions to support the secure management of TOE security functions and of TSF data such as the user security attributes and the audit trail upon which FIA and FAU class SFRs depend;
- SFRs from the FPT class provide appropriate protection of the TSF such as, protecting TSF data in transit (FPT_ITT.1 and FPT_ITT.3), blocking replay attacks (FPT_RPL.1), and supplying reliable time stamps (FPT_STM.1); and
- SFRs from the FCS class provide support to FAU and FPT class components by ensuring the confidentiality of binary data (IrisCodes and iris images) stored in the biometric database and ensuring the confidentiality and integrity of TSF data transferred between TOE components through 3DES encryption.

The dependency analysis provided at Table 19 and the analyses provided in Table 20, Table 21 and Table 22 demonstrate that the IT security functions work together to satisfy the TSFs, that is, they demonstrate mutual support between function components.

By definition, all assurance requirements support all SFRs since they provide confidence in the correct implementation and operation of the SFRs.

This analysis of the security functional and assurance requirements demonstrates that there are no conflicts between requirements. Therefore, the security requirements together form a mutually supportive and consistent whole.

8.3.4 Assurance Security Requirements Rationale

Table 23 below shows that all Security Assurance Requirements are met by the assurance measures.

Table 23: Mapping of SARs to Assurance Measures

Security Assurance Requirements	Assurance Measures
ACM_CAP.2	CM_DOC
ADO_DEL.1	DEL_DOC
ADO_IGS.1	IGS_DOC
ADV_FSP.1	FUN_SPEC
ADV_HLD.1	HLD_DOC
ADV_RCR.1	RCR_DOC
AGD_ADM.1	ADMIN
AGD_USR.1	USER
ATE_COV.1	TEST_COV
ATE_FUN.1	TEST_DOC
ATE_IND.2	TEST_DOC
AVA_SOF.1	SOF_DOC
AVA_VLA.1	VLA_DOC

Given that all Security Assurance Requirements are met by at least one Assurance Measure and that the implementation of each Assurance Measure will be the subject of evaluation activities, it is concluded that all of the Assurance Measures will meet all of the Security Assurance Requirements.

The primary function of the TOE is to provide identification and authentication of individuals based on their iris patterns. For consumers, the TOE is intended to replace existing unassured identification and authentication technologies (such as operating system password authentication mechanisms). As such, consumers may only require a low to moderate level of independently assured security for the identification and authentication services provided by the TOE. Further, for biometric technology, the strength of the functions providing for biometric identification, verification and enrolment of individuals are expressed in terms of FAR and FRR. Sufficient design information must be available for a statistical analysis of the strength of function.

CC-EAL2 provides design information down to the High-Level Design sufficient for the completion of an analysis of the strength of biometric functions, independent and developer testing of security functions and includes analysis of obvious vulnerabilities for the TOE. Therefore CC-EAL2 provides consumers with a low to moderate level of independently assured security services and is considered an appropriate level of assurance for the TOE.

8.3.5 Strength of function claims

At CC EAL-2, the TOE security assurance requirements include the AVA_SOF.1 component. The minimum strength of function (SOF) claim for the TOE SFRs is *SOF-basic*. Given the assurance level and the highly controlled nature of the TOE in its environment, the characteristics of the threats addressed by the TOE (Ref: 3.2.1) are limited to opportunistic attacks by users with little expertise, limited access to resources and low motivation. Therefore a claim of *SOF-basic* is appropriate.

A SOF claim is appropriate for all TOE security functions implementing the O.FARFRR security objective. This applies to the following TOE security functions:

- IDENTIFY;
- VERIFY;
- ENROL_ADD; and
- ENROL_DEL.

These TOE Security Functions implement the FIA_UAU.2 and FIA_UID.2 security functional requirements, which together provide the basis for biometric identification or verification of individuals based upon the their iris pattern. Biometric identification and verification are implemented by probabilistic mechanisms and the strength of these functions is usually expressed in terms of the false acceptance rate (FAR) and false rejection rate (FRR). Therefore, an explicit metric of FAR=1:1.1x10^6 and FRR=2:1x10^2 is claimed for these TOE Security Functions and is consistent with a claim of *SOF-basic*.

In addition to the above security functions, the TOE also implements a password-based mechanism for access to the maintenance application SYS_MAN (also implementing FIA_UAU.2 and FIA_UID.2 security functional requirements). Given the assurance level and the requirements for strong physical and logical environmental protection of the KnoWho Server, a claim of *SOF-basic* is appropriate for this TOE Security Function.

The function TRANS_SEC is implements FCS_COP.1. Determination of the strength of function for cryptographic algorithms is outside the scope of the CC. Therefore, no SOF claim is made for this TOE Security Function.

8.4 Rationale for Extensions

Not applicable.

8.5 PP Claims Rationale

This ST makes no PP conformance claim therefore no rationale is required.

Appendix A - Acronyms

CC	Common Criteria
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy