AUSTRALASIAN INFORMATION SECURITY EVALUATION PROGRAM

Certification Report

Certificate Number: 2003/26

SecureNet

TrustedNet Connect Version 2

Issue 1.0
May 2003

Issued by:

Defence Signals Directorate - Australasian Certification Authority

Executive Summary

This report describes the findings of the evaluation of SecureNet's TrustedNet Connect Version 2.0, developed by SecureNet Limited, to the Common Criteria (CC) Evaluation Assurance Level EAL4. The report concludes that the product has met the target assurance level of CC EAL4, and includes recommendations by the Australasian Certification Authority (ACA) that are specific to the secure use of the product. The evaluation was performed by CSC Australia and was completed on 31st January 2003.

TrustedNet Connect provides secure provision of key pair operations within a Public Key Infrastructure (PKI). The product consists of two major components:

- **Cardlets:** Software that is loaded and executed on a smart card, which are designed to protect, manage and control cryptographic keys stored on the smart card.

- **Host Software:** Software that interacts with the smart card and provides mechanisms to control and manage digital identifiers (digital IDs). The host software also provides Application Programming Interfaces (APIs) that provide end-user applications with a link to the card so that digital IDs can be accessed in a controlled manner.

TrustedNet Connect has been found to uphold the claims made in the Security Target (Ref [10]), and potential customers are urged to consult this document before planning to implement the product. In particular, TrustedNet Connect has been found to provide the claimed security functionality of user data protection, identification and authentication, and cryptographic support, when configured according to the evaluated configuration.

Ultimately, it is the responsibility of the user to ensure that TrustedNet Connect meets their requirements. For this reason, it is ***strongly*** recommended that prospective users of the product obtain a copy of the Security Target (Ref [10]) from the product vendor, and read this Certification Report thoroughly prior to deciding whether to purchase or implement the product.

Table of Contents

Chapter 1 Introduction

Intended Audience

This certification report states the outcome of the IT security evaluation of SecureNet's TrustedNet Connect. It is intended to assist potential users when judging the suitability of the product for their particular requirements.

This report should be read in conjunction with the Security Target for TrustedNet Connect (Ref [10]), which provides a full description of the security requirements and specifications that were used as the basis of the evaluation. A copy of the Security Target can be obtained from SecureNet.

Identification

Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to Chapter 7: Evaluated Configuration.

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	TrustedNet Connect Version 2.0
Software Version	TrustedNet Connect Server: Version 2.0.4.9 TrustedNet Connect PKCS#11 Provider: Version 2.0.4.9 TrustedNet Connect Microsoft CSP: Version 2.0.4.9 TrustedNet Connect Digital ID Cardlet: Version 2.0.4.9 TrustedNet Connect Key Management Cardlet: Version 2.0.4.9
Security Target	Security Target for SecureNet's TrustedNet Connect Version 2.0, Document Version 2.0 Revision 8, 29 January 2003
Protection Profile Claims	The Security Target does not claim conformance to a PP.
Evaluation Level	CC EAL 4
Conformance Result	CC Part 2 Conformant CC Part 3 Conformant
Evaluation Technical Report	Evaluation Technical Report for SecureNet's TrustedNet Connect 2.0, Version 2.0, 12 May 2003.
Version of CC	CC Version 2.1, August 1999
Version of CEM	CEM-99/045 Version 1.0, August 1999
Sponsor	SecureNet Limited
Developer	SecureNet Limited
Evaluation Facility	CSC Australia
Certifiers	Kirk Cheney, Chris Pennisi, Chris Clacher

Description of the TOE

The Target of Evaluation (TOE) is called TrustedNet Connect and its primary role is to store and control key pairs on behalf of the key pair owner. The key pairs are stored on smart cards. Public keys are conveyed between smart cards and certification authorities that must then associate them with the key pair owner—the smart card holder.

The certificates that the certification authority produces must be available at the server computer that relies on the public key for communication security. Certificates are inherently protected from modification and can be sent to the server from the client computer. For convenience, the TOE allows certificates to be stored on the smart card, allowing users to use their digital identities from any computer where TrustedNet Connect is installed.

TrustedNet Connect implements a number of APIs—including RSA Inc.'s PKCS#11 v2.1 and Microsoft's CSP Interface—that provide cryptographic services associated with the private key stored on a smart card. These APIs expose smart card functions for data decryption and digital signature operations, and they comply with published specifications. Compatible products exist for secure e-mail, SSL services, file encryption, transaction signing, IPsec clients, and smart card log on to computer systems.

The TOE is designed to be installed on workstations and accessed by interactive users. The operation of the TOE requires that a user be present to insert a smart card, and it is expected that the user control the host and applications through an interactive session.

For further information on the specific hardware and software components included in the evaluated configuration refer to Chapter 7: Evaluated Configuration, or Section 1.2 of the Security Target (Ref [10]).

Chapter 2 Security Policy

The TOE Security Policies (TSPs) define the security policies that the TOE must comply with in order to enforce the security functional requirements. The Security Target (Ref [10]) contains two explicit security policy statements Private Key SFP and Card Data SFP. In addition, the TOE implements a number of implied TSPs, drawn from the collection of security functional requirements. The TSPs are summarised as follows:

- **Identity and Authentication:** Users need to be identified in order to determine which assets are associated with them and to establish their rights to access data and cryptographic functions. Users are identified by the inserted smart card. Users identities are defined once a card is created with user specific information, including authentication data and user-specific cryptographic keys. The process of creating this information creates the user identity.

- **Access Control:** A discretionary access control policy is implemented on the smart card. Access rights or permissions are associated with controlled objects on the smart card so that operations on those objects by subjects are controlled according to object access rights.

- **Cryptography:** Encrypted information must remain confidential, and signatures must be unambiguously associated with the information that was signed. Cryptographic mechanisms must protect keys from disclosure. Cryptographic mechanisms are selected such that they are suitable to provide necessary security characteristics for the intended use of the functions that the mechanisms are applied.

- **Security Management:** The TOE effectively manages and controls security attributes associated with the TOE's access control policies. The TOE maintains the roles of issuer and user and enforces policy on static attribute initialisation.

- **Protection of the TSF:** If the TOE fails under any condition it will recover to a secure state without security compromise and will continue to enforce the TSP.

Chapter 3 Intended Environment for the TOE

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

Secure Usage Assumptions

The evaluation of the TrustedNet Connect product took into account the following assumptions about the secure usage of the TOE:

- The TOE is installed in an operating environment that is set up to protect the TOE from modifications and to withstand attacks by sophisticated external agents.
- The smart card is protected from disclosure of information through electromagnetic emanations and from physical attacks on the card.
- Public keys on smart cards are correctly associated with users' identities and distributed to relying parties; the association is revoked immediately when requested or when loss of the smart card is reported.
- Authorised TOE users and administrators are trusted to follow the guidance provided for secure operation of the TOE.
- Information which passes through smart card reader drivers and smart card readers to smart cards is not intercepted or modified.
- The OS on which the TOE is deployed correctly interfaces to the TOE.
- A trustworthy card operating system is used that loads card applications (cardlets) securely, protects them from other card applications, and erases all application data when they are deleted.

Clarification of Scope

The scope of the evaluation is limited to those claims made in the Security Target (Ref [10]). All security related claims in the Security Target were evaluated by CSC Australia as a component of the evaluation. A summary of the Security Target is provided in Appendix A of this Certification Report. The evaluated configuration for the TOE is provided in Chapter 7: Evaluated Configuration.

The TOE provides the following evaluated security functionality:

- **Cryptographic Services:** The implementation of cryptographic services on the card is based on functions provided by the smart card operating system. The on-card application uses these functions to implement cryptographic

services for: decrypting session keys, generating signatures, and decrypting private keys.

- **Identification and Authentication:** The TOE identifies users by their possession of a smart card on which their keys are stored. The TOE provides authentication by password that is associated with key slots.

- **Data Protection:** The TOE protects data contained on the smart card through the implementation of a discretionary access control policy that associates permissions with smart card objects and controls operations on those objects according to those object permissions.

- **Key Management:** The TOE provides the functionality to create and destroy RSA keys. The TOE can generate keys for use in certificate requests and for general signing purposes.

- **Password Management:** The TOE provides users with the ability to change their password. The TOE can implement a policy that restricts the numbers of times that password can be used and can require a minimum password length. A user password will be blocked if they enter their password incorrectly more times than a configurable number set by the issuer. The TOE also provides a one-time password facility, which is used to unblock a user's password.

- **Non-Repudiation:** The TOE provides the functionality for the user to accept responsibility for the authenticity of information. The TOE requires that the user confirm that the information being signed is that message that they are intending to send. This provides a mechanism for providing a guarantee of the validity of the data.

Potential users of the TOE are advised that the following **have not been evaluated** as part of the evaluation of TrustedNet Connect:

- Cryptographic functions implemented by Microsoft's CSP API or other CSPs with which the TOE may interact.

Chapter 4 TOE Architecture

TrustedNet Connect consists of the following major architectural components:

- **Host Software:** Software that interacts with the smart card and provides mechanisms to control and manage digital IDs. The host software also provides Application Programming Interfaces (APIs) that provide end-user applications with a link to the card so that digital IDs can be accessed in a controlled manner. The TrustedNet Connect host software includes the following:
    - **TrustedNet Connect Server**
    - **TrustedNet Connect PKCS#11 Provider**
    - **TrustedNet Connect Microsoft CSP Implementation**
- **Cardlets:** Software that is loaded and executed on a smart card, which are designed to protect, manage and control cryptographic keys stored on the smart card.
    - **TrustedNet Connect Digital ID Cardlet**
    - **TrustedNet Connect Key Management Cardlet**

The developer's high-level design identifies a number of functional subsystems of the TOE, which each implement a component of the security functionality. They are described as follows:

- **Management Console:** Provides functionality that enables the user to browse and configure the objects hosted by the server. The console makes use of the COM interfaces exposed by the server.
- **PKCS#11:** This subsystem implements a standardised interface used by client applications that require cryptographic functionality in line with the PKCS#11 standard.
- **MS Cryptographic Service Provider:** This subsystem implements a standardised interface used by client applications that require cryptographic functionality in line with Microsoft's CSP standard.
- **TrustedNet Connect COM Server:** Provides an object-oriented interface to the services provided by TrustedNet Connect. The server provides the implementation of the externally accessible COM interface.
- **Smart Card Component:** This subsystem keeps track of all smart cards that are visible to the system and provides the means to access the functionality they provide. This subsystem detects smart cards as they are inserted, determines the applications they contain, and then loads the appropriate drivers for processing the programmatic interface.

- **Key Store:** This subsystem defines a generic interface to a secure storage system and implements storage security features of the system, such as ensuring keys are stored under passwords with appropriate security properties and the caching of secure token state information.

- **Terminal Component:** This subsystem keeps track of all smart card terminals that are connected to the host platform. The subsystem configures the terminals and provides drivers that present a common interface for communication with the hosted smart card.

- **Key Generation:** This subsystem acts in tandem with the Digital ID subsystem to generate the private/public key data on the card.

- **Digital ID:** This subsystem provides a smart card based key storage implementation. This enables the private keys to be stored on the card and provides protection mechanisms. This subsystem also provides access functions for performing secure operations such as verifying passwords and data encryption.

Chapter 5 Documentation

It is important that TrustedNet Connect is used in accordance with the guidance documentation in order to ensure the secure usage of the TOE. SecureNet provides the following documents with the product:

- TrustedNet Connect Installation Guide, Version 2.0.4, Revision 2 (Ref [12])
- TrustedNet Connect Card Personaliser, Version 2.0.4, Revision 2 (Ref [13])
- TrustedNet Connect User Guide, Version 2.0.4, Revision 1, 20 August 2002 (Ref [14]).
- IssuerReadme.txt (included with issuer software), 29th January 2003 (Ref [15]).

The TrustedNet Connect Installation Guide (Ref [12]) is intended to provide the end-user with the guidance and information required to install and configure the TOE in a secure manner. The end-user is also supplied with the TrustedNet Connect User Guide (Ref [14]) to provide the effective guidance for operating the TOE in a secure manner.

The TrustedNet Connect Card Personaliser document (Ref [13]) is designed to provide the issuer with guidance for securely installing and configuring the TOE and issuing cards to end-users. Additionally, the text file, IssuerReadme.txt (Ref [15]) provides additional guidance to the issuer associated with the evaluated product.

Prior to receiving the product the issuer is also provided with the TrustedNet Connect 2: Delivery Instructions for Issuers (Ref [16]) document that provides guidance for the issuer when verifying the authenticity of the TOE.

Chapter 6 IT Product Testing

The objectives associated with the testing phase of evaluation can be placed into the following categories:

- **Functional testing:** Tests performed to ensure that the TOE operates according to its specification and is able to meet the requirements stated in the Security Target (Ref [10]).
- **Penetration testing:** Tests conducted to identify exploitable vulnerabilities in the TOE's intended operational environment.

Functional Testing

In this phase the evaluators analysed evidence of the developer's testing effort, including test coverage and depth analyses, test plans and procedures, and expected and actual results, to gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE. In addition, the evaluators drew on this evidence to develop a set of independent tests, comprising a sample of the developer tests, in order to verify that the test results matched those recorded by the developers, as well as a selection of independent functional tests that expanded on the testing done by the developers.

The functions tested covered the full range of Security Functional Requirements identified in the Security Target (Ref [10]), with the exception of those that rely on cryptographic operations. Whilst the tests devised did ensure that the cryptography was being implemented, testing of the actual cryptographic processes is considered the responsibility of the national cryptographic authority. In Australia, the cryptographic functions have been evaluated by the Defence Signals Directorate, as the national authority, and found suitable for Australian and New Zealand Government use. Australian and New Zealand Government users should carefully read the Cryptography section in Chapter 9: Recommendations.

Penetration Testing

The developers performed a vulnerability analysis of TrustedNet Connect, in order to identify any obvious vulnerabilities in the product and to show that they are not exploitable in the intended environment for the TOE. This analysis included a search for possible vulnerability sources in the evaluation deliverables, the intended TOE environment, public domain sources and internal SecureNet sources. A number of potential vulnerabilities relevant to the product type were identified and in each case the developers were able to show that the vulnerability was not exploitable on the TOE version of the product in the intended environment.

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

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

Chapter 7 Evaluated Configuration

The TOE is comprised of the following software components:

- TrustedNet Connect Server, Version 2.0.4.9
- TrustedNet Connect Digital ID Cardlet, Version 2.0.4.9
- TrustedNet Connect Key Management Cardlet, Version 2.0.4.9

The TOE requires the following hardware:

- An IBM-compatible PC (minimum Intel Pentium or compatible 166Mhz, 64 megabytes RAM, 10 megabytes hard disk space, a CDROM driver, and an available serial, PCMCIA, or USB port for a smart card reader). The PC must have the Windows 2000 Professional (Service Pack 2) operating system installed.
- A Keycorp MULTOS 4.02 (Release 1N'-AMD) E6 evaluated smart card, or
- A Keycorp MULTOS 4.06 (Release 1Q) smart card on Infineon SLE66CX320P.
- A Gemplus, or PC/SC compliant smart card reader, such as the Gemplus GemPC430.

Procedures for Determining the Evaluated Version of the TOE

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

For Issuers

A CD is prepared for issuers that contains the TrustedNet Connect software in self-expanding archives that are executables signed by SecureNet using Authenticode. Authenticode provides assurance of the identity of the publisher of the code, in this case SecureNet, and the codes integrity. More information on Authenticode can be obtained from Microsoft's website.

If encrypted smart card code is to be delivered, arrangements are made for a trusted representative of SecureNet to contact the issuer and install encryption keys.

Issuers will receive the CD with the TrustedNet Connect software through a courier service. Issuers should then follow the delivery instructions provided prior to delivery in the TrustedNet Connect 2: Delivery Instructions for Issuers (Ref [16]) document. This document provides the procedures that should be taken to: check the packaging of the software, check the authenticity of the software, and verify the authenticity of the Personaliser smart card.

If there are any problems encountered the issuer is requested to contact the SecureNet helpdesk.

For Users

End-users are also provided with guidance for verifying the authenticity of the TOE in the TrustedNet Connect Installation Guide (Ref [12]). The procedures provided check that SecureNet has created digital signatures and that the code is the code that was originally signed. It is the issuer's responsibility to ensure that the end-user receives properly personalised smart cards.

Chapter 8 Results of the Evaluation

Evaluation Procedures

The evaluation of TrustedNet Connect was conducted using the Common Criteria for Information Technology Security Evaluation (Refs [5] to [8]), under the procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [1] to [4]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [9]) were also upheld during the evaluation and certification of this product.

Certification Result

After due consideration of the Evaluation Technical Report (Ref [11]) produced by the evaluators and the conduct of the evaluation as witnessed by the certifiers, the Australasian Certification Authority has determined that TrustedNet Connect upholds the claims made in the Security Target (Ref [10]) and has met the requirements of the Common Criteria EAL4 assurance level.

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

Common Criteria EAL4

EAL4 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE, and a subset of the implementation, to understand the security behaviour. Assurance is additionally gained through an informal model of the TOE security policy.

The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, evidence of a developer search for vulnerabilities, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.

EAL4 also provides assurance through the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures.

A detailed explanation of the assurance requirements for EAL4 can be found in the Common Criteria, Part 3 (Ref [7]).

General Observations

The certifiers would like to acknowledge the invaluable assistance provided by CSC Australia and SecureNet Limited staff during the evaluation. The successful completion of this evaluation was made possible by their cooperation, technical assistance and attention to issues raised during the process.

Chapter 9 Recommendations

The following recommendations include information highlighted by the evaluators during their analysis of the developer's deliverables, during the conduct of the evaluation, and during the additional activities performed by the certifiers.

Scope of the Certificate

The certificate applies only to version 2.0.4.9 of the host and cardlet software on those hardware platforms identified in Chapter 7: Evaluated Configuration of this report. This certificate is only valid when TrustedNet Connect is installed and configured in its evaluated configuration as described in Chapter 7 and in accordance with the TrustedNet Connect Card Personaliser (Ref [13]) and TrustedNet Connect Installation Guidance (Ref [12]) documents.

TrustedNet Connect should only be used in accordance with the intended environment described in Chapter 3: Intended Environment for the TOE and Chapter 3 of the Security Target (Ref [10]).

Installation and Configuration Guide

Potential purchasers of the TOE are strongly recommended to review and follow all relevant installation and configuration guidance provided by SecureNet. Issuers should ensure that the TrustedNet Connect Card Personaliser document (Ref [13]) is used to install and configure the TOE in its evaluated configuration. Additionally, issuers should ensure that their end-users follow guidance provided in both the TrustedNet Connect Installation Guide (Ref [12]) and the TrustedNet Connect Users Guide (Ref [14]).

Smart Card Object Permissions

Issuers and users should be aware that when deleting a directory on a smart card only the delete permission on the directory applies and permissions associated with files within the directory are ignored. For example, when the permission relating to deleting a private key is set to "disabled" the private key cannot be deleted directly, however, if the permission on the key slot in which the private key has been created is set to "protected" or "enabled" the key slot can be deleted. Deleting the key slot will have the effect of removing both the key slot and any keys within that slot, even if the permission of the private key delete operation is set to "disabled."

If the issuer wants to ensure that the end-user cannot delete a private key on a smart card object then the permission on all directories that contain the private key, including the root directory, must be set to "disabled."

Cryptography

The evaluation of the cryptographic functions of TrustedNet Connect is beyond the scope of the Common Criteria evaluation, and has been undertaken as a separate process by the Defence Signals Directorate, the national cryptographic authority for

Australia. The cryptographic functions of TrustedNet Connect have been found to be suitable for Australian Government use, subject to the recommendations that follow.

TrustedNet Connect provides functionality for signing data and decrypting session keys using private keys on the smart card. When the TOE uses the TrustedNet Connect Microsoft CSP Implementation it passes symmetric key data encryption and decryption services through to Microsoft's Cryptographic Service Provider (CSP) API or a CSP that is able to handle the requested cryptographic function (Ref [17]). The purchaser must be aware that DSD's evaluation of the TrustedNet Connect's cryptographic functionality does not include the evaluation of cryptographic functions implemented by Microsoft's CSP API or other CSPs.

Purchasers of the product should be aware that the operating system for the TrustedNet Connect smart card is MULTOS 4.02 (Release 1N' – AMD) or MULTOS 4.06 (Release 1Q). MULTOS 4.02 (Release 1N' – AMD) has been evaluated under the AISEP to ITSEC E6, whereas, MULTOS 4.06 (Release 1Q) is currently in evaluation at ITSEC E6 and is due to be completed in the third quarter of 2003.

Australian and New Zealand Government users wishing to implement the TOE should take the following recommendations into account when planning their operational environment:

- **Key generation:** TrustedNet Connect uses RSA to generate key pairs. For Australian Government use, a key length of at least 1024 bits must be used.

- **Message digesting/hashing:** TrustedNet Connect supports both SHA-1 and MD5 as for digest calculation functions. For Australian Government use both SHA-1 and MD5 are approved, however, SHA-1 should be used in preference over MD5.

- **Digital signing and verification:** TrustedNet Connect supports RSA digital signing. RSA digital signing is approved for Australian government use provided a key length of at least 1024 bits is used. Additionally, the PKCS#1 format should be used in preference to the X.509 standard.

- **Encryption and decryption:** TrustedNet Connect performs RSA public key data encryption using the PKCS#1 and X.509 data encoding standards. RSA data encryption and decryption mechanisms are approved for Australian government use provided a key length of 1024 bits is used. The PKCS#1 data-encoding standard should be used in preference to the X.509 data encoding standard.

- **Wrapping and unwrapping session keys:** TrustedNet Connect performs key wrapping and unwrapping using the PKCS#1 data-encoding standard. The RSA session key wrapping function using the PKCS#1 data encoding format is approved for Australian government use provided a key of 1024 bits is used.

- **Random Number Generator (RNG):** The TOE has an RNG that is used in both the PKCS#11 API and Microsoft CSP API implementations. The

RNG was found to be appropriate for Australian government use, within the TrustedNet Connect product.

Appendix A Security Target Information

A brief summary of the Security Target (Ref [10]) is given below. Potential purchasers should obtain a copy of the full Security Target to ensure that the security enforcing functions meet the requirements of their security policy. A copy of the Security Target can be obtained from SecureNet.

Security Objectives for the TOE

TrustedNet Connect has the following IT Security Objectives:

- The TOE provides the means by which access to IT assets can be restricted.
- The cryptography implemented in the TOE is sufficient to withstand the cryptanalysis capabilities of likely attackers.
- When the non-repudiation key is used, the TOE provides users with means of checking the message to be signed. Users must then confirm the signing operation. The TOE checks that the generated signature matches the message to give users assurance that they are signing the intended message.
- The TOE uniquely identifies all users, and authenticates the claimed identity before granting users access to secure operations on protected IT assets.
- The TOE fully defines cryptographic components, functions, and interfaces to ensure appropriate protection for cryptographic keys throughout their life cycle, covering generation, distribution, storage, use, and destruction.
- The TOE ensures that there is no residual information in information containers or system resources used for passwords and secret cryptographic keys upon their re-allocation to different users.
- The TOE recovers to a secure state without security compromise after a system error or other interruption of system operation as a result of power interruptions.

Security Objectives for the Environment

TrustedNet Connect has the following IT Security Objectives for the environment:

- The operating environment is set up to protect the TOE from modification and is capable of resisting skilled attacks from external agents.
- The smart card is protected from disclosure of information through sufficiently low levels of electromagnetic emanations which correlate to

card information and resistance to physical attacks on the card (met by a MULTOS card).

- The correct associations between users and their public keys are distributed to relying parties and revoked in a timely manner.

- Those responsible for the configuration and operation of the TOE have read the provided guidance, and consequently shall set up and operate the TOE securely in accordance with the provided guidance.

- The third party smart card readers and drivers do not allow protected information to be read or interfered with and card readers and connectors are free of data interception devices.

- The OS on which the TOE is deployed correctly implements its published interfaces.

- The operating system on the smart card correctly implements cryptographic primitives and provides a source of random numbers with sufficient entropy that it will not reduce the effective length of cryptographic keys.

- The card operating system has been evaluated to at least an equivalent level as the TOE and protects card applications from disclosure or modification during loading, from interference from other card applications, and from disclosure of data after the application is deleted.

Threats

TrustedNet Connect addresses the following threats:

- An attacker may recover protected data through cryptanalysis or by exploiting any key management weakness.

- Protected secret data (secret cryptographic keys and passwords) may be revealed due to being kept in residual memory after the resource has been reallocated.

- Intentional or accidental power disruption may reveal protected information.

- The creator of a digitally signed message may deny having endorsed it.

- A person who is not authorised to use the TOE is able to obtain unauthorised access to TOE functionality or information protected by the TOE.

TrustedNet Connect has the following threats for the environment:

- Unauthorised users or skilled external agents exploit weaknesses in the operating environment to gain access to or modify the TOE.

- An attacker may successfully physically attack a smart card or analyse electromagnetic emanations to recover protected data stored on a smart card.

- The key material held on the smart card can be compromised during all stages of the card life-cycle resulting in an attacker either gaining unauthorised access to protected information on the card or disclosure of protected information. Attacks can occur at all stages of the smart card life-cycle from the manufacturer introducing malicious code to physical attacks on the card or attacks from other card applications once it has operational keys loaded onto it.

- Applications using the TOE incorrectly associate a user with a public key resulting in loss of information or authentication failure from man-in-the-middle attacks on the applications.

- An attacker may interfere with the operation of third party card readers or drivers to obtain protected information.

- User or configuration errors may leave the TOE in a state that is not secure, or may otherwise enable unauthorised persons access to the secure functions and/or protected information within the TOE.

- Failure of the OS on which the TOE is deployed to interface to the TOE correctly allows an unauthorised person to obtain protected information or access secure functions.

Summary of the TOE Security Functional Requirements

The TrustedNet Connect SFRs are given below. Full description of these SFRs can be found in Section 5.1 of the Security Target (Ref [10]).

- Class FCS: Cryptographic Support
  - FCS_CKM.1: Cryptographic key generation
  - FCS_CKM.4: Cryptographic key destruction
  - FCS_COP.1/RSA: Cryptographic operation
  - FCS_COP.1/Verify: Cryptographic operation
- Class FDP: User Data Protection
  - FDP_ACC.2/Keys: Complete access control
  - FDP_ACC.2/Card data: Complete access control
  - FDP_ACF.1/Keys: Security attribute based access control
  - FDP_ACF.1/Card data: Security attribute based access control

- FDP_ITC.1/Keys: Import of user data without security attributes
- FDP_ITC.1/Card data: Import of user data without security attributes
- FDP_DAU.2: Data authentication with identity of guarantor
- FDP_RIP.1: Subset residual information protection

- Class FIA: Identification and Authentication
  - FIA_AFL.1: Authentication failure handling
  - FIA_UAU.1: Timing of authentication
  - FIA_UAU.4: Single-use authentication mechanisms
  - FIA_UAU.6: Re-authenticating
  - FIA_UID.2: User identification before any action
- Class FMT: Security Management
  - FMT_MSA.1: Management of security attributes
  - FMT_MSA.2: Secure security attributes
  - FMT_MSA.3: Static attribute initialisation
  - FMT_SMR.1: Security roles
- Class FPT: Protection of the TSF
  - FPT_FLS.1: Failure with preservation of secure state

Security Requirements for the IT Environment

- Class FCS: Cryptographic Support
  - FCS_COP.1/Primitives: Cryptographic operation
  - FCS_COP.1/Random: Cryptographic operation

Security Requirements for the Non-IT Environment

None included.

Appendix B Acronyms

ACE	AISEP Certificate Extension
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
API	Application Programming Interface
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
COM	Common Object Model
CSP	Cryptographic Service Provider
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ITSEC	Information Technology Security Evaluation Criteria
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

Appendix C References

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

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

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

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

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

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

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

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

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

[10] SecureNet's TrustedNet Connect Version 2.0 Security Target Document Version 2.0 Revision 8
29 January 2003
SecureNet Limited

[11] SecureNet TrustedNet Connect Evaluation Technical Report (ETR) Version 2.0, 12 May 2003
CSC Australia
(EVALUATION-IN-CONFIDENCE)

[12] TrustedNet Connect Installation Guide
Version 2.0.4, Revision 2
SecureNet Limited

[13] TrustedNet Connect Card Personaliser
Version 2.0.4, Revision 2
SecureNet Limited

[14] TrustedNet Connect User Guide
Version 2.0.4, Revision 1, 20 August 2002
SecureNet Limited

[15] IssuerReadme.txt (included with issuer software)
29th January 2003
SecureNet Limited

[16] TrustedNet Connect 2: Delivery Instructions for Issuers (provided with contract)
SecureNet Limited

[17] TrustedNet Connect Cryptographic Service Provider API
Version 2.0.4, Revision 0
SecureNet Limited