Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

ActivCard Secure Remote Access
(Client V3.7.1, Server V4.2.1)

Certificate Number: 34/2005

October 2005

Version 1.0

Copyright Commonwealth of Australia 2005.

Reproduction is authorised provided that the report is copied in its entirety.

Amendment Record

Version	Date	Description
1.0	10/10/2005	Public Release

Executive Summary

1 This report describes the findings of the evaluation of ActivCard Developments Pty Ltd ActivCard Secure Remote Access product, to the Common Criteria Evaluation Assurance Level Two, EAL2. The Target of Evaluation (TOE), ActivCard Secure Remote Access, has met the target assurance level of EAL2. The evaluation was performed by CSC Australia and completed on 10 November 2004.

2 ActivCard Secure Remote Access is a product that is designed to act as a remote client to central concentrator Virtual Private Network (VPN) system with access intermediated via a service gateway. Once authenticated to the service gateway, the remote client is granted access to the business gateway, which allows encrypted access to the business applications required by the user.

3 The Australasian Certification Authority provides recommendations in this report that are specific to the secure use of the TOE. In addition, clarification of the scope of evaluation is provided and readers are informed of how to determine if the TOE is in its evaluated configuration.

4 It is recommended that end users ensure they maintain continuous oversight and control of their smart card during the course of a VPN session.

5 This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

6 Ultimately, it is the responsibility of the user to ensure that the ActivCard Secure Remote Access product meets their requirements. For this reason, it is recommended that a prospective user of the product refer to the Security Target at Ref [1] and read this certification report thoroughly prior to deciding whether to purchase the product.

7 Certification is not a guarantee of freedom from security vulnerabilities.

Table of Contents

Chapter 1 - Introduction

1.1 Overview

8 ActivCard Secure Remote Access, the Target of Evaluation (TOE), is a multi-component software package that provides Virtual Private Network (VPN) functionality. The TOE supports a model where remote clients initially connect to a service gateway (also known as the portal) for initial authentication. Once authenticated to the portal the remote client is granted access to the business gateway which acts as a VPN concentrator and thus allows encrypted access to the business applications required by the remote client user.

9 This report documents the Common Criteria (CC) evaluation and subsequent certification of the TOE.

1.2 Purpose

10 The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE against the requirements of the CC at Evaluation Assurance Level Two, EAL2, and

b) provide a source of detailed security information about the TOE for any interested parties.

11 The report should be read in conjunction with the TOE's Security Target (Ref [1]) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

12 Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to Section 2.5.1 Evaluated Configuration.

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	ActivCard Secure Remote Access
Software Version	ActivCard Remote Client V3.7.1 ActivCard Remote Server V4.2.1
Security Target	Security Target for ActivCard Secure Remote Access, Version 18, 2004.
Protection Profile Claims	N/A
Evaluation Level	CC EAL2
Conformance Result	CC Part 2 Conformant CC Part 3 Conformant
Evaluation Technical Report	ActivCard Secure Remote Access Evaluation Technical Report, Version 4.0, November 2004
Version of CC	CC Version 2.1, August 1999, Incorporated with Interpretations as of 14 May 2001.
Evaluation Methodology	CEM-99/045 Version 1.0, August 1999, Incorporated with Interpretations as of 14 May 2001.
Sponsor	ActivCard Developments Pty Ltd
Developer	ActivCard Developments Pty Ltd
Evaluation Facility	CSC Australia

Table 1 – Identification Information

Chapter 2 - Target of Evaluation

2.1 Description of the TOE

13 The TOE is the ActivCard Secure Remote Access VPN product developed by ActivCard Developments Pty Ltd. Its primary role is to allow remote users to securely access their organisation's computer network over an insecure network. The TOE's general security functions are authentication, access control, cryptography, misuse warnings, audit functions and anti-replay security.

14 The three main components of the TOE are the client (user) software, the service gateway (also known as the portal) and the business gateway. Secure communications between the three entities (client, portal and business gateway) are ensured through use of the IPSec protocol to provide secure Encapsulated Security Payload (ESP) tunnel-mode encryption and authentication over insecure networks.

15 The user of the TOE must be in possession of a smart card, which holds their public certificate and private key and is accessed by a PIN. The client software provides an interface to the smart card, as well as implementing IPSec on behalf of the user. The client software obtains the certificate from the smart card. On presentation of the certificate to the portal, the user is verified via the Lightweight Directory Access Protocol (LDAP) before being allowed to make a connection to the business gateway. The user can access the business gateway via an Internet connection or by dialling directly to the dial-up Remote Authentication Dial-In User Service (RADIUS) system.

16 Once the portal has verified the user, the client software is permitted to establish an IPSec tunnel with the business gateway. The business gateway confirms with the portal that the user has been verified for access before allowing the client to access the business system.

17 For further information on the specific hardware and software components included in the evaluation configuration refer to Section 2.5.1 Evaluated Configuration.

2.2 TOE Architecture

18 The TOE consists of the following major architectural components:

a) **Client software**: Provides an interface to the smart card, as well as implementing IPSec on behalf of the user. Can be connected to the portal via a dial-up modem or can connect to the portal and business gateway via an Internet connection.

b) **Service gateway (portal)**: Verifies the user, once a user is verified it allows for an IPSec tunnel to be established between the client

software and the business gateway. It is made up of a RADIUS server to support dial-in connections, a Domain Name System (DNS) server and a portal server.

c) **Business gateway**: Confirms with the portal that a user had been verified before allowing the client software to access the business system.

2.3 Clarification of Scope

19 The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]).

2.3.1 Evaluated Functionality.

20 The TOE provides the following evaluated security functionality:

a) **Authentication:** The user is authenticated to the smart card and to server components of the TOE (portal, RADIUS server and business gateway) to ensure the user's identity.

b) **Access control:** Successful authentication results in the user gaining access to the organisational resources protected by the business gateway. User attributes and organisational settings are used to determine what access will be granted.

c) **Cryptography:** The TOE is capable of cryptographic functions, which provide support to the authentication, confidentiality and integrity features.

d) **Confidentiality:** Communications over insecure networks are protected from disclosure through encryption.

e) **Integrity:** IPSec protects communications over insecure networks from modification.

f) **Misuse warning:** The TOE will present a warning/misuse banner to all users, and will not allow further access until the user accepts the conditions of the banner.

g) **Audit:** Security relevant events are recorded at the portal and business gateway.

h) **Privacy:** No user information will be transmitted across an insecure network, that is, a secure communications channel is established before user information is sent.

i) **Anti-replay:** The RADIUS server will reject authentication attempts which contain data previously used to successfully authenticate the user.

2.3.2 Non-evaluated Functionality

21 Potential users of the TOE are advised that a set of functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration. The functions and services that are part of the product and have not been included as part of the evaluation are provided below.

a) **RDBMS:** The Security Target mentions the possible use of a Relational Database Management System (RDBMS) for storing audit data. This was not evaluated.

b) **Firewall:** The TOE does not provide firewall functionality.

c) **LDAP:** The TOE does not provide the LDAP directory service.

2.4 Security Policy

22 The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected. The TSP is defined in the Security Target (Ref [1]). A summary of the TSP is provided below:

a) **Security audit:** The ability to generate audit records and then associate them with the identity of the user that caused the event is provided by the TOE. Only administrators of the TOE will have the capability to access the audit logs.

b) **Cryptographic support:** Cryptographic operations are implemented to support data encryption/decryption, digital signature verification, key agreement and hashing. Encryption algorithms and key sizes are chosen to provide maximum available protection for the data being encrypted.

c) **User data protection:** The TOE security functions enforce access control to objects based on an IP address and user X.509 certificate, PIN or username and password.

d) **Identification and authentication:** Administrators and users need to be identified and authenticated before they can undertake any action. This is done via the use of one or more of the following attributes: X.509 certificate, PIN, private key and sequence number (for RADIUS dialup access).

e) **Privacy:** The TOE ensures that all agents are unable to determine the real user name bound to initial client – portal communications prior to the establishment of an IPSec session.

f) **Protection of the TOE security functions:** The ability to detect sequence number anomalies in dialup RADIUS access has been implemented within the TOE. When a sequence number out of order is detected the physical link will be dropped and the client will be informed of a dial error.

g) **TOE access:** Before the establishment of a user session an advisory warning message regarding unauthorised use of the TOE will be shown to the user.

h) **Trusted path/channels:** Communication channels between the TOE security functions and remote trusted clients are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.

2.5 Usage

2.5.1 Evaluated Configuration

23 This section describes the configurations of the TOE that were included within scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in these defined evaluated configuration(s). The evaluated configuration is listed below in Table 2.

TOE Component	Specifications
Client Workstation	
Computing Platform	A PC with CD-ROM and LAN or Modem connectivity able to run one of the operating systems listed below: • Windows 98 Second Edition • Windows NT4 with Service Pack 5 • Windows 2000 Professional with Service Pack 2 or 4 • Windows XP with no Service Pack
TOE Software	ActivCard Remote Client V3.7.1
Smart Card Reader	The following smart card readers were used: • GemPlus GemPC410 Serial • ActivCard SmartReader serial (ACTR-01) • ActivCard 201 PCMCIA (SCR201) • ActivCard 301 USB (SRR200) (Note: Serial readers require a 9-pin COM port for the data connection and a PS/2 port for power.)
Business Gateway	
Computing Platform	Ultra 5, Netra-T1 or V100 2 Network Interfaces. Operating System: Sun Solaris 8 with *Solaris 8 Recommended Patch Cluster version 15 August 2003*. (File: 8_Recommended.zip, Size: 93475078, MD5: 31d7fe15bd8553b9511c27266d76da2f)
TOE Software	ActivCard Remote Server V4.2.1
Portal / RADIUS Server	
Computing platform	As per Business Gateway

TOE Software	ActivCard Remote Server V4.2.1
Smart Card	
Computing Platform	MULTOS 1Q (Keycorp) including AMD with ID

Table 2 – Evaluated Configuration

2.5.2 Determining the Evaluated Configuration

24 The server administrator or client software user can verify the version of the software that they are running at any time. The server software was released on 8 Sep 2003 and the CD is labelled 4.2.1[0]. On the server computers the software version can be determined by running the Solaris command "pkginfo –x ACTI*Package_Name"* command where ACTI is prepended to the *Package_Name* identifier listed in Table 3 below.

Package Name	Business Gateway Version	Portal/RADIUS Server Version
abizl		4.2.1.0
agate	4.2.1.0	4.2.1.0
arad		4.2.1.0
disec	5.0.0.3	5.0.0.3
aimon	4.1.0.1	4.1.0.1
tcert	4.1.0.0	4.1.0.0
lstdc	2.10.0.0	2.10.0.0
mautm	2.0.5	2.0.5

Table 3 – Configuration of Servers

25 The client software version can be checked by inspection of the client interface. It should be titled V3.7.1.1.

2.5.3 Delivery Procedures

26 When placing an order for ActivCard Secure Remote Access customers should make it clear to ActivCard that they wish to receive the evaluated product.

27 ActivCard Developments Pty Ltd has a set of procedures to ensure that the integrity of the TOE is maintained throughout the delivery process. Before the hardware is shipped to the customer, a fax is sent to the customer confirming their order. This fax includes the serial numbers and identifying characteristics (make, model, operating system versions) of all hardware and installed software that is to be shipped to the customer.

28 In most cases an ActivCard Engineer will personally deliver the product and is responsible for examining the tamper-evident seals upon the boxes received to ensure integrity. If a courier is used for delivery, the fax sent advises the customer to examine the tamper-evident seals on all boxes received to verify seal integrity. The customer will also be advised not to open the boxes or tamper with the seals until an ActivCard Engineer is on site to verify the hardware.

29 After initial installation of the hardware the ActivCard Engineer is responsible for checking the serial numbers and identifying characteristics (make, model, operating system versions) of the hardware to ensure it is consistent with the packages that were shipped from ActivCard. If the seals have been tampered with or the version and serial numbers do not match the fax received by the customer, the entire shipment should be returned to ActivCard for rebuilding.

2.5.4 Documentation

30 It is important that ActivCard Secure Remote Access is used in accordance with the guidance documentation in order to ensure the secure usage of the TOE.

31 The evaluated user guidance documentation is Secure Remote Access (SRA) User Guide, Version 7, 14 June 2004 (Ref [2]).

32 The evaluated administrator guidance is listed below.

a) Secure Remote Access Gateway Administration Guide for Version 4.2.1, Version 9, 19 January 2004 (Ref [3]).

b) IAS Provider, IAS Installation Guide, Version 6, 12 January 2004 (Ref [4]).

c) ActivCard SRA Gateway Configuration Reference Guide for Version 4.1, Commercial In Confidence, Issue 9, 20 November 2002 (Ref [5]).

d) ActivCard SRA Business Locator Configuration Reference Guide for Version 4.1.3, Commercial In Confidence, Issue 8, 20 November 2002 (Ref [6]).

e) ActivCard SRA Audit Configuration Reference Guide for Version 4.1, Commercial In Confidence, Issue 7, 20 November 2002 (Ref [7]).

f) ActivCard SRA RADIUS Configuration Reference Guide, Version 7, 20 November 2002 (Ref [8]).

The primary administrator guidance resource document is Secure Remote Access Gateway Administration Guide for Version 4.2.1, Version 9, 19

January 2004 (Ref [3]). This is the key document for clarifying TOE aspects such as configuring DNS, the portal, RADIUS server and the business gateway.

2.5.5 Secure Usage

33 The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must be upheld in order to ensure the security objectives of the TOE are met.

34 The following assumptions were made:

a) The portal and business gateway components are protected by an appropriate firewall from un-trusted networks.

b) Only trusted agents have logical access to the server components of the TOE (portal, business gateway, RADIUS server). This may be implemented by the trusted agent having an operating system account that has access to the TOE software.

c) The server components of the TOE are located in a physically secure environment. This means only trusted persons can physically access these components.

d) The valid owner of the smart card is the only person who can gain physical access to the smart card and knows the correct PIN.

e) The TOE will have access to the services of an evaluated smart card to provide cryptographic and storage facilities.

Chapter 3 - Evaluation

3.1 Evaluation Procedures

35 The evaluation of the TOE was conducted using the Common Criteria for Information Technology Security Evaluation (Refs [9],[10],[11],[12]) under the procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [13],[14],[15],[16]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [17]) were also upheld during the evaluation and certification of the product.

3.2 Functional Testing

36 In this phase the evaluators analysed evidence of the developer's testing effort, including test coverage, 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 perform a sample of the developer tests in order to verify that the test results matched those recorded by the developers. The functional testing effort also included a selection of independent functional tests that expanded on the testing done by the developers.

3.3 Penetration Testing

37 The developer performed a vulnerability analysis of ActivCard Secure Remote Access, in order to identify any obvious vulnerability in the product and to show that the vulnerability is not exploitable in the intended environment of the TOE. This analysis included a search for possible vulnerability sources in the evaluation deliverables, the intended TOE environment, public domain sources and internal ActivCard Developments Pty Ltd sources. The developer identified a number of potential vulnerabilities relevant to the product type and in each case the developer was able to show that the vulnerability was not exploitable in the TOE's intended operational environment.

38 Based on the information given in the developer's vulnerability analysis, the evaluators were able to devise a penetration test plan. After the completion of testing, the evaluators were able to determine that the TOE, in its intended environment, utilising the recommendation in this report, has no obvious exploitable vulnerabilities.

Chapter 4 - Certification

4.1 Certification Result

39 After due consideration of the conduct of the evaluation as witnessed by the certifiers, and of the Evaluation Technical Report (Ref [18]) the Australasian Certification Authority certifies the evaluation of ActivCard Secure Remote Access performed by CSC Australia.

40 The evaluators found that ActivCard Secure Remote Access upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the CC EAL2 assurance level.

41 Certification is not a guarantee of freedom from security vulnerabilities.

4.2 Assurance Level Information

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

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

44 EAL2 also provides assurance through a configuration list for the TOE, and evidence of secure delivery procedures.

4.3 Recommendations

45 To avoid exploitation of residual vulnerabilities discovered during the evaluation it is very important that the client machines (including the smart card reader) are physically secure and are continuously controlled by the user for the duration of each secure VPN session. For secure operation the end-user must always be in control of their smart card and should not allow others to insert or remove their smart card or to interfere with the smart card reader.

Annex A. References and Abbreviations

A.1. References

[1] Secure Remote Access Security Target, Version 18, 2004.

[2] Secure Remote Access (SRA) User Guide, Version 7, 14 June 2004.

[3] Secure Remote Access Gateway Administration Guide for Version 4.2.1, Version 9, 19 January 2004.

[4] IAS Provider, IAS Installation Guide, Version 6, 12 January 2004.

[5] ActivCard SRA Gateway Configuration Reference Guide for Version 4.1, Commercial In Confidence, Issue 9, 20 November 2002.

[6] ActivCard SRA Business Locator Configuration Reference Guide for Version 4.1.3, Commercial In Confidence, Issue 8, 20 November 2002.

[7] ActivCard SRA Audit Configuration Reference Guide for Version 4.1, Commercial In Confidence, Issue 7, 20 November 2002.

[8] ActivCard SRA RADIUS Configuration Reference Guide, Version 7, 20 November 2002.

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

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

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

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

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

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

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

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

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

[18] ActivCard Secure Remote Access Evaluation Technical Report, Version 4.0, November 2004, CSC Australia. (EVALUATION-IN-CONFIDENCE)

A.2. Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CC	Common Criteria
CEM	Common Evaluation Methodology
DNS	Domain Name System
EAL	Evaluation Assurance Level
ESP	Encapsulated Security Payload
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest #5
RADIUS	Remote Authentication Dial-In User Service
RDBMS	Relational Database Management System
SRA	Secure Remote Access
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
VPN	Virtual Private Network