Secure Remote Access Security Target

for

ActivCard Developments Pty Ltd

Document version: 18
Document status: Released

List of Tables

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 requirements; refinement, selection, assignment and iteration are defined in Section 2.1.4 of Part 2 of the CC.

Terminology

In the CC, many terms are defined in Section 2.3 of Part 1. The following terms are a subset of those definitions. They are listed here to aid the user of the Security Target.

AES	Advanced Encryption Standard implemented by Rijndael algorithm
Business Gateway	TOE component at customer site that provides secure access of business resources to Client over insecure network
CC	Common Criteria
Client	Combination of the end-user and end-user software
EAL	Evaluation Assurance Level
IAS	Internet Authentication Service
IPSec	Internet Protocol Security. Secure network communication standard.
OSP	Organisational Security Policy
Portal	TOE component used to authenticate Client access
PP	Protection Profile
RADIUS	Remote Authentication Dial-In User Service. Protocol and software authenticating dial-in users.
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
SRA	Secure Remote Access. The components which make up the TOE.
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
TSS	TOE Summary Specification
TTP	Trusted Third Party

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. This section includes the rationale for the defined security objectives.

Section 5 contains the functional requirements derived from the Common Criteria, Part 2 that must be satisfied by the TOE. This section includes the security requirements of the environment and the rationale for all functional requirements.

Section 6 provides the TOE Summary Specification, which describes the TOE functions in TOE specific terms. Included in this section is the rationale showing that these functions are suitable to satisfy the functional requirements of section 5.

Section 7 contains a reference to the assurance requirements from the Common Criteria, Part 3 that must be satisfied by the TOE. The assurance measures taken by the developer and the appropriate rationales are contained in this section.

A reference section (Section 8, Annex A) is provided to identify background material.

1 Introduction

1.1 Identification

Title:	Secure Remote Access Security Target
Authors:	CSC
ST Version:	18
Document status	Draft
TOE Version:	ActivCard Secure Remote Access Client v3.7.1 and ActivCard Secure Remote Access Server v4.2.1
CC Version:	2.1
General Status:	Not released

1.2 Security Target Overview

This Security Target describes the security requirements, functionality, environment and assurance measures relating to the Target of Evaluation (TOE) defined by this document. This Security Target is a baseline reference document for the evaluation and certification of the TOE. The audience this document is aimed at certifiers, evaluators and includes potential customers of the product, and they should have an understanding of Public Key Infrastructure, encryption, Virtual Private Networks and IPSec.

The TOE is ActivCard's Secure Remote Access (SRA) suite of software, which allows remote users to securely access their organisation's computer network and resources, over an insecure network. The user can connect by dialling up or through an internet connection. The user's identity is authenticated before access is granted to the organisation's network. SRA uses the Internet Protocol Security (IPSec) standard to encrypt the user's communication providing confidentiality and integrity of the data transmitted. In this sense the TOE provides Virtual Private Network (VPN) functionality.

Assurance of the user's identity and strength of the data encryption is implemented using Public Key Infrastructure (PKI) and smart cards. Users are authenticated to the Service Gateway or Portal before establishing a secure connection to their Business Gateway. However the costs to initially set up a PKI can be expensive, which is why ActivCard.com can provide the necessary PKI authentication provided by the Portal as a service to customers who are interested in this TOE.

This TOE encompasses end user access to business resources via ActivCard's SRA. Management of the smart cards used in SRA is described in [1], which is also a basis for Common Criteria evaluation.

1.3 Conformance Claim

The TOE is conformant with Parts 2 and 3 of the CC (Version 2.1), and will conform to EAL2 measures in CC Part 3.

2 Target of Evaluation

This part of the ST shall describe the TOE as an aid to the understanding of its security requirements, and shall address the product or system type. The scope and boundaries of the TOE shall be described in general terms both in a physical way (hardware and/or software components/modules) and a logical way (IT and security features offered by the TOE).

The TOE description provides context for the evaluation. The information presented in the TOE description will be used in the course of the evaluation to identify inconsistencies. If the TOE is a product or system whose primary function is security, this part of the ST may be used to describe the wider application context into which such a TOE will fit.

2.1 Product Type

Secure Remote Access (SRA) components form a Virtual Private Network, allowing remote users to securely access their organisation's computer networks over an insecure network.

2.2 General TOE Functionality

The TOE's general security functions are Authentication, Access Control, Cryptography (providing Authentication, Confidentiality and Integrity), Misuse warnings, Audit functions and Anti-Replay security.[1]

The three main components of the TOE are Client (user) software, the Service Gateway (also known as Portal) and the Business Gateway. Secure end-to-end transactions between the three entities (Client, Portal, Business Gateway) are ensured through use of the SSH IPSec protocol for secure tunnel-mode encryption and authentication over insecure networks.

The user of the TOE will be in possession of a smart card, which holds his public certificate and private key and is accessed by a PIN. The smart card provides secure cryptographic functionality, the Operating System of which has been previously evaluated to a level at least equivalent to that of this TOE (this way the smart card can be trusted to operate securely). The Client software provides an interface to the smart card, as well as implementing the IPSec operations on behalf of the user. The Client can access their business resources via an Internet connection or by dialling directly to the Dial-Up RADIUS server. On presentation of the certificate to the Portal, the user is verified via LDAP before being allowed to make a connection to the Business Gateway.

ActivCard typically manages the Portal on behalf of the customer, however the customer may install and maintain a portal in their own environment if they desire.

Business Gateways available to the user are negotiated with the business in question, typically the user will be an employee who requires secure remote access to the business' e-commerce infrastructure.

Once the Portal has verified the user, the Client 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.

[1] Further details regarding the functionality of the TOE can be found in section 2.3.2

IPSec provides confidentiality of the transmitted data via encryption. Integrity of the transmitted data is implemented by IPSec ensuring that the data has not been modified during transmission.

Other security features of the TOE which contribute to ensuring the remote access is secure are:

The TOE provides a comprehensive audit trail of events that occur from using secure remote access. These events record the person’s identity and TCP/IP address (where applicable) to provide accountability of actions. The audit trail will provide evidence that can be used to detect if TOE security is undermined.

The TOE will present a misuse / warning banner to all users attempting to gain access to a business gateway. The user has to accept the banner’s conditions before access is granted.

The Dial-Up RADIUS server can detect and prevent replay attacks.

The user’s identity is never transmitted unencrypted over an insecure network.

2.3 Scope and Boundaries

It is important to define the scope and boundaries of the TOE so that the components and modules are properly evaluated and certified. Figure 1 – TOE Boundary depicts a block diagram of the scope of the TOE, while the boundary is indicated by the solid thick line. The Dialup and Network clouds represent the insecure networks and do not fall into the scope of the TOE. The Directory and RDBMS structures also fall outside the scope of the TOE. Each of the shaded blocks represents a component of the TOE. The client components include a smart card (and reader) that contains the user's X.509 certificate and private key.

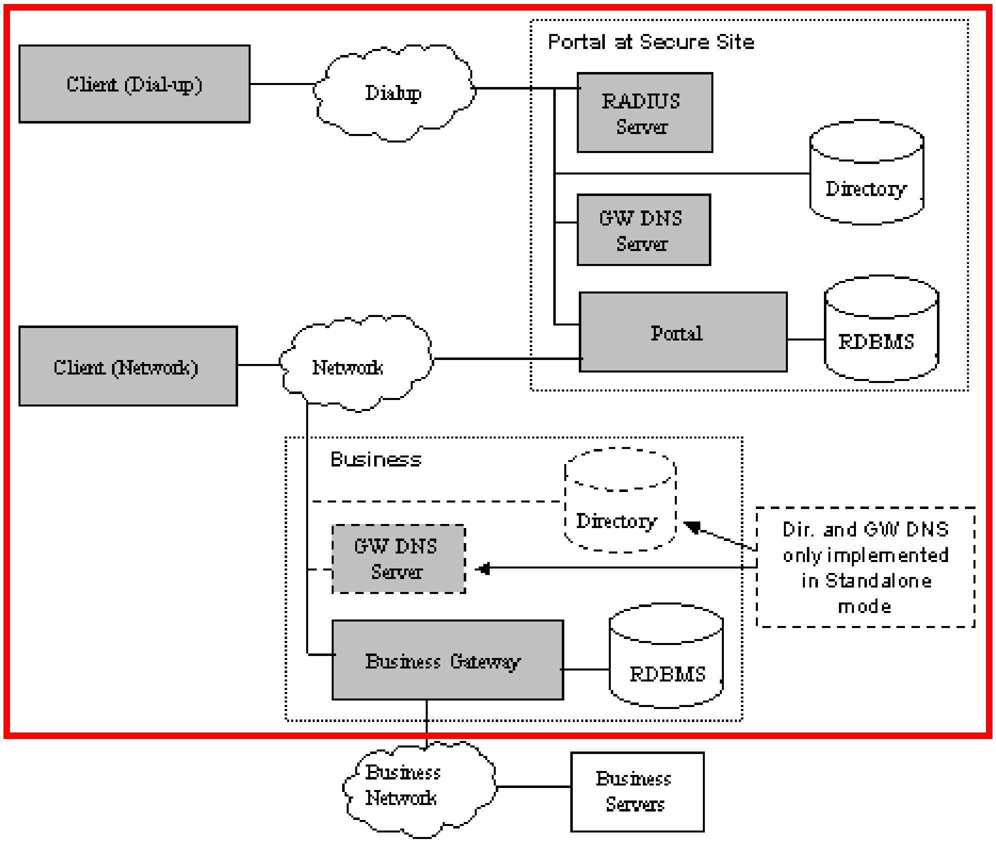

Figure 1 – TOE Boundary

2.3.1 Physical Scope and Boundaries

Table 2-1 TOE components lists the physical components and versions that compose the TOE.

TOE Component	Specifications
Client Workstation	
TOE Software	ActivCard Remote Client V3.7.1

PC	A PC with a CDROM driver running one of the following: • Windows 98 Second Edition • Windows NT4 with Service Pack 5 or 6A • Windows 2000 with Service Pack 2 or 3 • Windows XP with no Service Pack or Service Pack 1 Minimum of Pentium-133 with 32MB of RAM. LAN/Modem connectivity (ie, NIC or modem)
Hardware	A smart card reader is required. The following are supported: • GemPlus GemPC410 Serial • Utimaco CardMan 4000 PCMCIA • ActivCard SmartReader serial (ACTR-01) • ActivCard 201 PCMCIA (SCR201) • ActivCard 301 USB (SRR200) • Serial readers require a 9-pin COM port for the data connection and a PS/2 port for power.
Business Gateway	
PC	Ultra 5, Netra-T1 or V100. No minimum specifications but RAM will affect encryption performance while processor will affect Security Associations performance. 2 Network Interface Cards (NICS) will be required.
Operating System	Sun Solaris 8 with *Solaris 8 Recommended Patch Cluster version 15 August 2003*. **File: 8_Recommended.zip** **MD5: 31d7fe15bd8553b9511c27266d76da2f** **Size: 93475078** IP enabled.
TOE Software	ActivCard Remote Server V4.2.1
Hardware	No extra hardware required.
Portal	
PC	As per Business Gateway
Operating System	As per Business Gateway
TOE Software	ActivCard Remote Server V4.2.1
Hardware	No extra hardware required.
RADIUS Server	
PC	As per Business Gateway (Can be the same server as used for the portal gateway.)
Operating System	As per Business Gateway
TOE Software	ActivCard Remote Server V4.2.1

Hardware	No extra hardware required
GW DNS Server	
	The GW DNS service is a standard Solaris service configured for SRA. This service typically runs on the Portal Gateway machine. This service is implemented by the “bind” application. If this is required at the Business site, then it runs in a machine separate from the Business Gateway.
Smart Card	
Physical Card and operating system	The physical smart card and operating system should be evaluated to at least the same level as this TOE. Example: MULTOS 1Q including AMD with ID (0020v003) on Infineon Technologies SLE66CX160P or SLE66CX320P Smartcard Integrated Circuits. MULTOS 1Q implements version 4.06 of the MULTOS specification.
TOE Software	No additional software is required on the smart card.

Table 2-1 TOE components

The TOE requires any LDAP version 3 compliant directory server for the X.509 certificates.

2.3.2 Logical Scope and Boundaries

The security features offered by the TOE make up the logical scope and boundary. The security features are:

Authentication: The user is authenticated to the smart card and to server components of the TOE (Portal, RADIUS and Business Gateway) to ensure the user’s identity.

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 the granting of access.

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

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

Integrity: IPSec protects communications over insecure networks from modification.

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.

Audit: Security relevant events are recorded at the Portal and Business Gateway.

Privacy: No user information will be transmitted across an insecure network before a secure communications channel is established.

Anti-Replay: The RADIUS authenticator will reject authentication attempts, which contain data previously used to successfully authenticate the user.

3 TOE Security Environment

This section defines the security problem that the TOE and its environment is intended to address. This consists of the assumptions made relevant to secure usage of the TOE, the threats the TOE and environment will counter and the organisational policies with which the TOE and environment shall comply.

3.1 Secure Usage Assumptions

Assumption	Description
A.Firewall: Firewall Protection	The Portal, Business Gateway components are protected by an appropriate firewall from untrusted networks.
A.Logical: Logical Access	Only trusted agents have logical access to the server components of the TOE (Portal, Business Gateway, RADIUS). This may be implemented by the trusted agent having an operating system account that has access to the TOE software.
A.Physical: Physical Security	The server components of the TOE (ie. not client PC) are located in a physically secure environment. This means only trusted agents can physically access these components.
A.Owner_PIN Only owner has card and PIN	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.
A.Evaluated_Smartcard Services of evaluated Smartcard	The TOE will have access to the services of an evaluated smart card to provide cryptographic and storage facilities

Table 3-1 - Secure Usage Assumptions

3.2 Threats to Security

Threats may be addressed by either the TOE or its environment (eg, using personnel, physical or administrative safeguards). Potential attackers are assumed to have only public knowledge of the TOE, use standard computer equipment, have a proficient knowledge of TCP/IP, cannot gain access to server components of the TOE, but may access client application. This equates to a Low level of attack strength.

Threat	Description
T.Card_Access: Smart Card Access	An agent may get unauthorised logical access to protected information stored upon the smart card. An agent may get unauthorised logical access to protected services provided by the smart card.
T.Privacy: User information revealed	A user's information may be revealed upon an untrusted network prior to establishing a secure connection.
T.Replay: Re-use of Dialup authentication data	An agent may use previously valid authentication data to gain access to protected services via the Dial-up service.
T.Service_Access:	An attacker may gain unauthorised remote logical access to

Unauthorised access to services	protected services.
T.Trans-Disclosure: Transmitted Information Disclosure	Protected transmitted information may be disclosed to unauthorised agents.
T.Trans-Modify: Modification of Transmitted Information	Unauthorised agents may modify protected transmitted information.
T.Undetected: Security events not recorded.	Security related events occurring at the RADIUS, Portal and Business Gateway may not be recorded, resulting in security related actions not being detected. Recorded information relating to remote user access provide a means to detect actions performed by the TOE. If meaningful information relating to remote user access are not recorded then actions by attackers or authorised users cannot be detected. This could result in protected business services being accessed without detection.
T.Warning: Misuse / Warning Banner	An agent may access a service without viewing and accepting the Misuse / Warning text related to that particular service.

Table 3-2 – Threats

Env Threat	Description
TE.Card_Privacy:	Assets on smart card may be compromised, or disclosed to unauthorised agents.

Table 3-3 - Environmental Threats

3.3 Organisational Security Policies

Organisational Security Policies	Description
P.Password: Smart Card Password Policy	The client software can be set to ensure the password restrictions for the smart card meet the organisation's requirements for passwords

Table 3-4 - Organisational Security Policies

4 Security Objectives

This section defines the security objectives that the TOE and environment shall uphold. These objectives will be suitable to counter all threats identified in the previous section.

4.1 *Security Objectives for the TOE*

Objective	Description
O.Access: Access Control	The TOE shall provide secure remote access to protected services to allowed users.
O.Audit: Audit	The TOE will record all security related events occurring at the RADIUS, Portal and Business Gateway components, allowing detection of security related actions.
O.Banner: Warning	The TOE has the facility to display Misuse / Warning text informing users about the services they are accessing.
O.Card_Security: Security of Smart Card	The TOE shall ensure the logical security of the protected information on the smart card is maintained.
O.Comms: Communications	The TOE shall ensure that protected information is securely transmitted across untrusted networks.
O.Crypt: Cryptography	The TOE shall perform cryptographic operations to provide security of protected transmitted information and identification and authentication of entities
O.I&A: Identification and Authentication	The TOE shall ensure a user is identified and authenticated before allowing access to protected services and information.
O.Privacy: User Privacy before secure session	The TOE shall ensure that user information is kept private before a secure communications channel is established.
O.Replay: Replay for Dialup	For Dialup mode, the TOE shall prevent an agent from re-using valid authentication data to gain access to protected services.

Table 4-1 – Security Objectives for the TOE

4.2 *Security Objectives for the Environment*

OE.Card_Protection:	The assets are stored on the smart card will be protected from physical disclosure and modification. This will be enforced by the evaluated smart card operating system.
OE.Secure_Servers	The server components of the TOE (Portal, Business Gateway, RADIUS) are to have a secure environment. This includes firewall protection from untrusted networks, secure physical location, and logical access controls to be in place.
OE.Trusted_PIN:	The presentation of the correct PIN to the smart card means the user is the valid owner of the card and the PIN can be trusted.

Table 4-2 - Security Objectives for the Environment

4.3 Security Objectives Rationale

Table 4-3 shows that all threats, assumptions and policies are mapped to at least one security objective, and vice versa. This means that all threats, assumptions and policies are covered and that the security objectives are necessary.

	O.I&A	O.Card_Security	O.Privacy	O.Replay	O.Access	O.Crypt	O.Audit	O.Banner	O.Comms	OE.Card_Protection	OE.Secure_servers	OE.Trusted_PIN
TE.Card_Privacy										✓		
T.Card_Access	✓	✓										✓
T.Privacy			✓									
T.Replay				✓								
T.Service_Access	✓				✓	✓					✓	
T.Trans-Disclosure						✓			✓			
T.Trans-Modify						✓			✓			
T.Undetected							✓					
T.Warning								✓				
A.Firewall											✓	
A.Logical											✓	
A.Physical											✓	
A.Owner_PIN												✓
A.Evaluated_Smartcard										✓		
P.Password		✓										

Table 4-3- Mapping the TOE Security Environment to Security Objectives

4.3.1 Rationale for countering threats

The following sub-sections provide rationales justifying that each threat is suitably countered by the security objectives that are mapped to it.

T.Card_Access: Smart Card Access

An agent may get unauthorised access to protected information stored upon the smart card. An agent may get unauthorised access to protected services provided by the smart card.

In General, T.Card_Access is addressed by:

- **O.I&A: Identification and Authentication**: the TOE shall ensure a user is identified and authenticated before allowing access to protected services and information. This will ensure that only authorised users can gain access to the protected information and services upon the smart card.
- **O.Card_Security**: the TOE shall ensure the logical security of the protected information on the smart card is maintained. The software components of the TOE, in conjunction with the I&A objective will restrict logical access of smart card assets to only authorised authenticated users. This aids in stopping unauthorised agents gaining logical smart card access.
- **OE**.**Trusted_PIN**: Only the valid owner will be presenting the correct PIN for the smart card. An unauthorised agent will not have access to the correct PIN and physical access to the smart card. This way if an attacker has access to one they will not be able to get to information or services protected by the smart card.

T.Privacy: User information revealed

A user's information may be revealed upon an untrusted network prior to establishing a secure connection.

In General, T.Privacy is addressed by:

- **O.Privacy:** The TOE shall ensure that user information is kept private before a secure communications channel is established. No user information shall be transmitted before a secure IPSec session is established, therefore cancelling the threat of user’s information being revealed upon an untrusted network.

T.Replay: Re-use of Dialup authentication data

An agent may use previously valid authentication data to gain access to protected services via the Dial-up service.

In General, T.Replay is addressed by:

- **O.Replay:** For Dialup mode, the TOE shall prevent an agent from re-using valid authentication data to gain access to protected services. This will directly cancel the threat of a replay attack using old authentication data.

T.Service_Access: Unauthorised access to services

An attacker may gain unauthorised remote logical access to protected services.

In General, T.Service_Access is addressed by:

- **O.Access**: The TOE shall provide secure remote access to protected services to allowed users. User attributes will determine access to protected services. An authorised user will gain access while unauthorised users will not have access granted. This will contribute to stopping unauthorised access to protected services.
- **O.Crypt**: The TOE shall perform cryptographic operations to provide security of protected transmitted information and identification and authentication of entities. Cryptographic operations are used to determine a users authority to gain access to protected services. This will contribute to establishing a user’s identity and authorisation and stopping unauthorised access.
- **O.I&A**: The TOE shall ensure a user is identified and authenticated before allowing access to protected services and information. Every user is identified and authenticated before access is granted. Some cryptographic operations contribute

to achieving this objective. All three objectives will, in conjunction, stop unauthorised access to protected services.

- **OE**.**Secure_servers**: The secure environment around the server components of the TOE will reduce the attacker's opportunity to access the servers and therefore the protected services.

T.Trans-Disclosure: Transmitted Information Disclosure

Protected transmitted information may be disclosed to unauthorised agents.

In General, T.Trans-Disclosure is addressed by:

- **O.Comms**: The TOE shall ensure that protected information is securely transmitted across untrusted networks. Using the IPSec tunnels to secure a communications channel between the Client and the Business Gateway will reduce the likelihood of information being disclosed.
- **O.Crypt**: The TOE shall perform cryptographic operations to provide security of protected transmitted information and identification and authentication of entities. Encryption of data in the IPSec tunnels will make the transmitted data unreadable, reducing the likelihood of the information being disclosed to unauthorised agents.

T.Trans-Modify: Modification of Transmitted Information

Protected transmitted information may be modified by unauthorised agents.

In General, T.Trans-Modify is addressed by:

- **O.Comms**: The TOE shall ensure that protected information is securely transmitted across untrusted networks. Using the IPSec tunnels to secure a communications channel between the Client and the Business Gateway will reduce the likelihood of information being modified.
- **O.Crypt**: The TOE shall perform cryptographic operations to provide security of protected transmitted information and identification and authentication of entities. Integrity checking of data in the IPSec tunnels will reduce the likelihood of the information being modified by unauthorised agents.

T.Undetected: Security events not recorded.

Security related events occurring at the RADIUS, Portal and Business Gateway may not be recorded, resulting in security related actions not being detected.

In General, T.Undetected is addressed by:

- **O.Audit**: The TOE will record all security related events occurring at the RADIUS, Portal and Business Gateway components, allowing detection of security related actions. With security-related events recorded, trusted agents will be able to review the events and determine the security implications of the events. This will reduce the likelihood of security events being undetected.

T.Warning: Misuse / Warning Banner

An agent may access a service without viewing and accepting the Misuse / Warning text related to that particular service.

In General, T.Warning is addressed by:

- **O.Banner**: The TOE has the facility to display Misuse / Warning text informing users about the services they are accessing. This will inform agents/users of the services they are accessing, and must accept the conditions before continuing. This will cancel the threat that agents were not aware of the services accessed.

TE.Card_Privacy:

Assets on smart card may be compromised, or disclosed to unauthorised agents.

In General, TE.Card_Privacy is addressed by:

- **OE.Card_Protection**: The assets stored on the smart card will be protected from physical disclosure and modification. This will be enforced by the evaluated smart card operating system. An evaluated smart card operating system will provide assurance that access controls cannot be bypassed by unauthorised agents to disclose or modify assets on the smart card, thereby cancelling this threat.

4.3.2 Rationale of assumption support

A.Firewall: Firewall Protection

The Portal and Business Gateway components are protected by an appropriate firewall from untrusted networks.

In general, A.Firewall supports:

- **OE**.**Secure_servers**: The firewall(s) in place support the protection of the TOE from unauthorised clients and attackers by providing a first line of defence screening incoming transmissions.

A.Logical: Logical Access

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

In general, A.Logical supports:

- **OE**.**Secure_servers**: Only trusted agents have logical access to the server components of the TOE. This restricts access to the logical components of the TOE via which an untrusted agent may gain unauthorised access to the protected services of the TOE.

A.Physical: Physical Security

The server components of the TOE (ie. not client PC) are located in a physically secure environment. This means only trusted agents can physically access these components.

In general, A.Physical supports:

- **OE**.**Secure_servers**: The server components of the TOE (ie. not client PC) are located in a physically secure environment. This restricts access to the physical components of the TOE via which an untrusted agent may gain unauthorised access to the protected services of the TOE.

A.Owner_PIN: Only owner has both card and PIN

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.

In general, A.Owner_PIN supports:

- **OE.Trusted_PIN**: Presentation of the correct PIN indicates that the user has knowledge of the PIN and physical access to the card. As the valid owner of the card is the only person to have both these, then the PIN can be trusted as not be from an unauthorised agent.

A.Evaluated_Smartcard: services of evaluated Smartcard

The TOE relies on the services of an evaluated smart card to provide secure cryptographic and storage facilities. The evaluated smart card is protected from disclosure of information through electromagnetic emanations and from physical attacks on the card.

In general, A.Evaluated_Smartcard supports:

- **OE.Card_Protection**: The TOE will have access to the services of an evaluated smart card to provide cryptographic and storage facilities

4.3.3 Policy Rationale

P.Password: Smart Card Password Policy

The client software can be set to ensure the password restrictions for the smart card meet the organisation's requirements for passwords.

In general, P.Password supports:

- **O.Card_Security**: The TOE shall ensure security of the protected information on the smart card is maintained by specifying a minimum strength of PIN selected by the user.

5 IT Security Requirements

5.1 TOE Security Functional Requirements

All the Security Functional Requirements (SFRs) in this section were drawn from CC Part 2 functional requirements components with the operations completed. All standard CC text is in regular font, whereas the text inserted (assignment and selection) for this ST is underlined. Refinements to the SFRs are indicated by **bold characters** when new text added and ~~strikethrough~~ when text is removed. Iterations are identified by a number in brackets (#) following the SFR being iterated.

5.1.1 Security audit (FAU)

Audit data generation (FAU_GEN.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;

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

c) Events as provided in section 6.1.8.$^{\text{FAU\_GEN.1.1}}$

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 ~~PP/~~ST, IP Address and Gateway Identity is also recorded.$^{\text{FAU\_GEN.1.2}}$

User identity association (FAU_GEN.2)

The TSF shall be able to associate each auditable event with the identity of the user that caused the event.$^{\text{FAU\_GEN.2.1}}$

Audit review (FAU_SAR.1)

The TSF shall provide Administrators with the capability to read all audit events as listed in section 6.1.8 from the audit records.$^{\text{FAU\_SAR.1.1}}$
The TSF shall provide the audit records in a manner suitable for the user to interpret the information.$^{\text{FAU\_SAR.1.2}}$

Restricted audit review (FAU_SAR.2)

The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access. $^{\text{FAU\_SAR.2.1}}$

5.1.2 Cryptographic support (FCS)

Cryptographic key generation (FCS_CKM.1)

The TSF shall generate cryptographic keys in accordance with ~~a~~ specified cryptographic key generation algorithms:

1. 3DES;
2. AES

and specified cryptographic key sizes:

1. 192
2. 128, 192, 256

that meet the following:

1. RFC 2405
2. RFC 3394 [FCS_CKM.1.1]

Cryptographic key distribution (FCS_CKM.2)

The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method Diffie-Hellman that meets the following: PKCS#3. [FCS_CKM.2.1]

Cryptographic key destruction (FCS_CKM.4)

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method zeroisation that meets the following: [none].[FCS_CKM.4.1]

Cryptographic operation (FCS_COP.1)

The TSF shall perform

1. Data Encryption/Decryption
2. Data Encryption/Decryption
3. Digital Signature and Verification
4. Key Agreement
5. Hashing

in accordance with ~~a~~ specified cryptographic algorithms:

1. 3DES CBC;
2. AES;
3. RSA;
4. Diffie-Hellman;
5. SHA 1;

and cryptographic key sizes:

1. 192 (3DES);
2. 128, 192, 256 (AES)
3. 1024
4. 1024 (ISAKMP Group-2)
5. Not applicable (SHA 1)

that meet the following:

1. RFC 2405
2. RFC 3394
3. RFC 2409
4. PKCS#3
5. RFC 2104[FCS_COP.1.1]

5.1.3 User data protection (FDP)

Subset access control (FDP_ACC.1)(1)

The TSF shall enforce the Portal Access Control SFP on

Subject:	Client, Portal and Business Gateway
Objects:	Internal protected hosts
Operations:	IPSec network access.[FDP_ACC.1.1]

Security attribute based access control (FDP_ACF.1)(1)

The TSF shall enforce the Portal Access Control SFP to objects based on IP Address and user X.509 Certificate.[FDP_ACF.1.1]

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

The Client's IP Address is an allowed value

An LDAP lookup of the user's certificate determines the user's access [FDP_ACF.1.2]

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

A user has to be authenticated at the Portal via LDAP and have an entry in the Portal's Active Client Register before the Business Gateway will establish a secure connection with the Client. Once a secure session is established the user can securely access the protected hosts. [FDP_ACF.1.3]

The TSF shall explicitly deny access of subjects to objects based on the

status attribute in Portal User directory is NOT set to ENABLED/ACTIVE OR

the user does not accept the misuse / warning message presented.[FDP_ACF.1.4]

Subset access control (FDP_ACC.1)(2)

The TSF shall enforce the Client Access Control SFP on

Subject:	Smart card, Client Software
Objects:	Smart card information
Operations:	Access of information on Smart card.[FDP_ACC.1.1]

Security attribute based access control (FDP_ACF.1)(2)

The TSF shall enforce the Client Access Control SFP to objects based on PIN.[FDP_ACF.1.1]

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: the client software is still active and while the smart card is "unlocked" (ie the PIN has been presented).[FDP_ACF.1.2]

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: user can edit password of smart card. This allows organisation policy to be

followed when changing password.$^{\text{FDP\_ACF.1.3}}$
The TSF shall explicitly deny access of subjects to objects based on the none.$^{\text{FDP\_ACF.1.4}}$

Subset access control (FDP_ACC.1)(3)

The TSF shall enforce the Dialup Access Control SFP on

Subject:	Dialup Client, RADIUS Authenticator
Objects:	Internal protected hosts
Operations:	Remote modem access.$^{\text{FDP\_ACC.1.1}}$

Security attribute based access control (FDP_ACF.1)(3)

The TSF shall enforce the Dialup Access Control SFP to objects based on User X.509 Certificate details.$^{\text{FDP\_ACF.1.1}}$
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: if the username and password presented to the RADIUS Authenticator is valid. $^{\text{FDP\_ACF.1.2}}$

Application Note: The Client generates the username from the serial number, issuer hash of CA and Distinguished Name (DN) stored on the smart card. The password is generated the sequence number and digital signature stored on the smart card.

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

The sequence number presented in the password is greater than the previous value used in authentication AND

An LDAP lookup of the user's certificate determines the user's access.$^{\text{FDP\_ACF.1.3}}$

The TSF shall explicitly deny access of subjects to objects based on the

if the sequence number contained in the password is equal or less than server recorded at previous authentication.$^{\text{FDP\_ACF.1.4}}$

Complete information flow control (FDP_IFC.2)

The TSF shall enforce the Information Flow Control SFP on:

Subject:	Client, Business Gateway
Information:	Protected Internal information

And all operations that cause that information to flow to and from subjects covered by the SFP.$^{\text{FDP\_IFC.2.1}}$
The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.$^{\text{FDP\_IFC.2.2}}$

Simple security attributes (FDP_IFF.1)

The TSF shall enforce the Information Flow Control SFP based on the following types of subject and information security attributes: IP Address, IPSec parameters.$^{\text{FDP\_IFF.1.1}}$
The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

The Client's IP Address is an allowed value AND

The Client and Business Gateway can agree on IPSec parameters$^{\text{FDP\_IFF.1.2}}$

The TSF shall enforce ~~the~~ Phase 1 Security Association, Phase 2 Security Association, key life expiration.$^{\text{FDP\_IFF.1.3}}$

The TSF shall provide the following: IPSec functionality.[FDP_IFF.1.4]

The TSF shall explicitly authorise an information flow based on the following rules:

The requesting Client user must have been authenticated as per Portal Access Control SFP or the Dialup Access Control SFP.[FDP_IFF.1.5]

The TSF shall explicitly deny an information flow based on the following rules:

if Business Gateway IP filter set to explicitly "deny host" for the Client IP address.[FDP_IFF.1.6]

Basic internal transfer protection (FDP_ITT.1)

The TSF shall enforce the Information Flow Control SFP to prevent the disclosure, modification of user data when it is transmitted between physically-separated parts of the TOE.[FDP_ITT.1.1]

5.1.4 Identification and authentication (FIA)

Authentication failure handling (FIA_AFL.1)

The TSF shall detect when 3 unsuccessful authentication attempts occur related to sending PIN to card.[FIA_AFL.1.1]

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall block card.[FIA_AFL.1.2]

User attribute definition (FIA_ATD.1)

The TSF shall maintain the following list of security attributes belonging to individual users:

X.509 certificate (on smart card and in LDAP);

PIN (on card);

Private Key (on card for signing during authentication);

Sequence number (on card and at RADIUS for Dial up access). [FIA_ATD.1.1]

Timing of authentication (FIA_UAU.1)(1) *

The TSF shall allow the user to select a Portal to connect to, present the misuse / warning banner to the user and negotiate Phase 1 IPSec on behalf of the user to be performed before the user is authenticated.[FIA_UAU.1.1]

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.[FIA_UAU.1.2]

* This SFR relates to Portal Authentication only. The TOE requires two types of authentication – authentication to the smart card, and authentication to the Portal.

Timing of authentication (FIA_UAU.1)(2) *

The TSF shall allow unprotected information on the smart card to be presented (as in line with PKCS #11) on behalf of the user to be performed before the user is authenticated.[FIA_UAU.1.1]

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.[FIA_UAU.1.2]

* This SFR relates to card authentication only.

Protected authentication feedback (FIA_UAU.7) *

The TSF shall provide only asterisks "*" to the user while the authentication is in progress.[FIA_UAU.7.1]

* This SFR relates to card authentication only.

Timing of identification (FIA_UID.1)(1) *

The TSF shall allow DNS lookup, presentation of the misuse / warning banner to the user and initiation of Phase 1 negotiations on behalf of the user to be performed before the user is identified.[FIA_UID.1.1]
The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.[FIA_UID.1.2]

* This SFR relates to Portal identification only. The TOE requires two types of identification – identification to the smart card, and identification to the Portal.

Timing of identification (FIA_UID.1)(2) *

The TSF shall allow the user to select the Portal to connect to on behalf of the user to be performed before the user is identified.[FIA_UID.1.1]
The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.[FIA_UID.1.2]

* This SFR relates to Card identification only.

5.1.5 Privacy (FPR)

Anonymity (FPR_ANO.1)

The TSF shall ensure that all agents are unable to determine the real user name bound to initial Client – Portal communications prior to establishing IPSec session.[FPR_ANO.1.1]

* This SFR relates to Main Mode (default) configuration for IPSec only.

5.1.6 Protection of the TOE Security Functions (FPT)

Replay detection (FPT_RPL.1)

The TSF shall detect replay for the following entities: sequence number in dialup RADIUS access.[FPT_RPL.1.1]
The TSF shall perform

> RADIUS authenticator will reject the Radius authentication, which will inform the originating NAS (Network Access Server) to drop the physical link to the client; the Client will get a RAS dial error

when replay is detected.[FPT_RPL.1.2]

5.1.7 TOE access (FTA)

Default TOE access banners (FTA_TAB.1)

Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.[FTA_TAB.1.1]

5.1.8 Trusted path/channels (FTP)

Inter-TSF trusted channel (FTP_ITC.1)

The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.[FTP_ITC.1.1]
The TSF shall permit the TSF to initiate communication via the trusted channel.[FTP_ITC.1.2]
The TSF shall initiate communication via the trusted channel for the Business Gateway needs to verify the user is still in the Portal's Active Client Register. [FTP_ITC.1.3]

5.2 *IT Security Requirements for the IT Environment*

The TOE has no EXPLICITLY STATED security requirements allocated to it.

5.3 *Security Functional Requirements Rationale*

Objectives	Requirements
O.Access	FDP_ACC.1(1), FDP_ACF.1(1), FDP_ACF.1(3), FDP_ACC.1(3),
O.Audit	FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2
O.Banner	FTA_TAB.1
O.Card_Security	FDP_ACC.1(2), FDP_ACF.1(2), FIA_AFL.1, FIA_ATD.1, FIA_UAU.1(2), FIA_UID.1(2), FIA_UAU.7
O.Comms	FTP_ITC.1, FDP_IFC.2, FDP_IFF.1, FDP_ITT.1,
O.Crypt	FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1
O.I&A	FDP_ACC.1(1), FDP_ACF.1(1), FDP_ACC.1(2), FDP_ACF.1(2), FDP_ACC.1(3), FDP_ACF.1(3), FIA_AFL.1, FIA_ATD.1, FIA_UAU.1(1), FIA_UID.1(1) FTP_ITC.1
O.Privacy	FPR_ANO.1
O.Replay	FPT_RPL.1

Table 5-1 – Mapping the Security Functional requirements to the Security Objectives

5.3.1 O.Access: Access Control

The TOE shall provide secure remote access to protected services to allowed users .

O.Access is implemented in the TOE by:

- FDP_ACC.1(1): Subset access control; which defines the subjects (client, portal and business gateway), objects (internal protected hosts) and operations (IPSec network access) between which there is an access control policy.
- FDP_ACF.1(1): Security attribute based access control; which defines the rules which must be applied to the subjects and objects for the operations defined in FDP_ACC.1(1). In this case, user must appear in the active user register before the Business Gateway will establish a connection with him.
- FDP_ACC.1(3): Subset access control; which defines the subjects (Dialup Client, RADIUS Authenticator), objects (internal protected hosts) and operations (remote modem access) between which there is an access control policy.

- FDP_ACF.1(3): Security attribute based access control; which defines the rules which must be applied to the subjects and objects for the operations defined in FDP_ACC.1(3). In this case, The sequence number presented in the password is greater than the previous value used in authentication, and an LDAP lookup of the user's certificate is used to determine the user's access.

Together, these SFRs provide secure remote access to allowed users of the TOE.

5.3.2 O.Audit: Audit

The TOE will record all security related events occurring at the RADIUS, Portal and Business Gateway components, allowing detection of security related actions.

O.Audit is implemented in the TOE by:

- FAU_GEN.1: Audit data generation; which generates audit events for all security related events, as specified in section 6.1.8
- FAU_GEN.2: User identity association; which associates a user identity with each security related event in the TOE.
- FAU_SAR.1: Audit review; which provides and administrator with the ability to review the audit records to determine whether a security breach has occurred.
- FAU_SAR.2: Restricted audit review; which restricts access to the audit logs to those users explicitly granted read-access, to prevent the unauthorised alteration of audit records.

Together, these SFRs provide the ability to audit all security related events in the TOE..

5.3.3 O.Banner: Banner Warning

The TOE has the facility to display Misuse / Warning text informing users about the services they are accessing.

O.Banner is implemented in the TOE by:

- FTA_TAB.1: Default TOE access banners; which displays the misuse/warning banner for the portal to which the user is connecting, and displays other warning banners for the business gateway if required.

FTA_TAB.1 provides the entirety of the functionality required by O.Banner.

5.3.4 O.Card_Security: Security of Smart Card

The TOE shall ensure security of the protected information on the smart card is maintained.

O.Card_Security is implemented in the TOE by:

- FDP_ACC.1(2): Subset access control; which defines the subjects (smart card, client software), objects (smart card information) and operations (access of information on smart card) between which there is an access control policy.
- FDP_ACF.1(2): Security attribute based access control; which defines the rules which must be applied to the subjects and objects for the operations defined in FDP_ACC.1(2). In this case, the client software must be active and the smart card must be unlocked.
- FIA_AFL.1: Authentication failure handling; which locks the smart card after three unsuccessful PIN entry attempts.

- FIA_ATD.1: User attribute definition; which maintains the X.509 certificate, PIN and private key on the card for the purposes of signing and authentication.
- FIA_UAU.1(2): Timing of authentication; which allows the user to perform a limited number of actions before being authenticated to the card, such as obtaining the location of the business locator from the portal.
- FIA_UID.1(2): Timing of identification; which allows the client to select a portal to connect to before being positively identified by the card.
- FIA_UAU.7: Protected authentication feedback; which protects the user PIN by obscuring it when entered into the client interface.

Together, these SFRs ensure the security of the information on the smart card.

5.3.5 O.Comms: Communications

The TOE shall ensure that protected information is securely transmitted across untrusted networks.

O.Comms is implemented in the TOE by:

- FTP_ITC.1: Inter-TSF trusted channel; which negotiates and maintains a secure tunnel between the Business Gateway and Portal for the transmission of secure encrypted data regarding the Active Client Register.
- FDP_IFC.2: Complete information flow control; which ensures that all information flows between the Client and the Gateway are controlled by the Information Flow Control policy.
- FDP_IFF.1: Simple security attributes; which defines the rules which must be applied to the subjects and objects for the operations defined in FDP_IFC.2. In this case, the client IP address must be allowed by the filter, and the client must be set to accept the Gateway settings as negotiated with it.
- FDP_ITT.1: Basic internal transfer protection; which enforces the portal access control and information flow control policies, to prevent disclosure and modification of the user data during transmission between physically separate parts of the TOE.

Together, these SFRs ensure that information is securely transmitted across untrusted networks between the TOE components.

5.3.6 O.Crypt: Cryptography

The TOE shall perform cryptographic operations to provide security of protected transmitted and information identification and authentication of entities.

O.Crypt is implemented in the TOE by:

- FCS_CKM.1: Cryptographic key generation; which is used by the TOE for IPSec tunnel negotiation, and identification and authentication of entities.
- FCS_CKM.2: Cryptographic key distribution; which is used to distribute keys during the IPSec negotiation process.
- FCS_CKM.4: Cryptographic key destruction; which is used to destroy keys generated by the TOE after they are no longer required, using zeroisation.
- FCS_COP.1: Cryptographic operation; which controls the cryptographic operations (data encryption/decryption, digital signature verification, IPSec negotiation and hashing) using trusted algorithms and key sizes.

Together, these SFRs provide all the cryptographic functionality for the TOE.

5.3.7 O.I&A: Identification and Authentication

The TOE shall ensure a user is identified and authenticated before allowing access to protected services and information.

O.I&A is implemented in the TOE by:

- FDP_ACC.1(1): Subset access control; which defines the subjects (client, portal and business gateway), objects (internal protected hosts) and operations (IPSec network access) between which there is an access control policy.
- FDP_ACF.1(1): Security attribute based access control; which defines the rules which must be applied to the subjects and objects for the operations defined in FDP_ACC.1(1). In this case, user must appear in the active user register before the Business Gateway will establish a connection with him.
- FDP_ACC.1(2): Subset access control; which defines the subjects (smart card, client software), objects (smart card information) and operations (access of information on smart card) between which there is an access control policy.
- FDP_ACF.1(2): Security attribute based access control; which defines the rules which must be applied to the subjects and objects for the operations defined in FDP_ACC.1(2). In this case, the client software must be active and the smart card must be unlocked.
- FDP_ACC.1(3): Subset access control; which defines the subjects (Dialup Client, RADIUS Authenticator), objects (internal protected hosts) and operations (remote modem access) between which there is an access control policy.
- FDP_ACF.1(3): Security attribute based access control; which defines the rules which must be applied to the subjects and objects for the operations defined in FDP_ACC.1(3). In this case, The sequence number presented in the password is greater than the previous value used in authentication, and an LDAP lookup of the user's certificate is used to determine the user's access.
- FIA_AFL.1: Authentication failure handling; which locks the smart card after three unsuccessful PIN entry attempts.
- FIA_ATD.1: User attribute definition; which maintains the X.509 certificate, PIN and private key on the card for the purposes of signing and authentication.
- FIA_UAU.1(1): Timing of authentication; which allows the user to perform a limited number of actions before being authenticated to the portal, such as connecting and negotiating Phase 1 IPSec.
- FIA_UID.1(1): Timing of identification; which allows the client to perform Phase 1 IPSec negotiation with the portal before being positively identified by the portal.
- FTP_ITC.1: Inter-TSF trusted channel; which allows the Business Gateway to check the Portal's Active Client Register to verify the user has been authenticated at the Portal.

Together, these SFRs ensure that users are identified and authenticated before being allowed access to protected services and information.

5.3.8 O.Privacy: User Privacy before secure session

The TOE shall ensure that user information is kept private before a secure communications channel is established.

O.Privacy is implemented in the TOE by:

- FPR_ANO.1: Anonymity; which obscures the identity of the user from being transmitted during the initial communications between the Client and the Portal, before an IPSec session has been established.

5.3.9 O.Replay: Replay for Dialup

For Dialup mode, the TOE shall prevent an agent from re-using valid authentication data to gain access to protected services.

O.Replay is implemented in the TOE by:

- FPT_RPL.1: Replay detection; which detects the re-occurrence of sequence numbers in RADIUS dialup, which can indicate a replay attack.

5.4 Mutual Support Security Requirements

The purpose of this rationale is to show that the IT security requirements (and the SFRs in particular) are complete and internally consistent by demonstrating that they are mutually supportive and provide an 'integrated and effective whole'.

Dependency helps in showing mutual support because if SFR-A is dependent on SFR-B then by definition, SFR-B is supportive of SFR-A.

This ST is targeting a standard EAL 2 assurance package and so the dependency and mutual support of the assurance requirements is self-evident as the EAL is taken from the CC.

For those SFRs not directly related by dependency, mutual support can be provided by SFRs which address the following:

5.4.1.1 Help prevent bypassing of other SFRs

The iterations of FIA_UID.1 and FIA_UAU.1 support other functions which allow the user access to the assets by restricting the actions the user can take before being authorised.

The user has to accept the access banner (FTA_TAB.1) before being allowed access as determined by the Portal Access Control SFP (FDP_ACF.1 (1) and FDP_ACC.1 (1)). Acceptance of the banner cannot be bypassed.

To ensure that a user has not bypassed authentication by the Portal, the Business Gateway verifies with the Portal all users requesting access have been authenticated. The TOE uses a trusted channel (FTP_ITC.1) to verify the authentication.

5.4.1.2 Help prevent tampering of other SFRs

The cryptographic functions FCS_CKM.1, FCS_CKM.2, FCS_CKM.4 and FCS_COP.1 provide for the secure generation, handling, destruction and operation of keys, and therefore support those SFRs which may rely on the use of those keys.

The iterations of FIA_UID.1 and FIA_UAU.1 support other functions which allow the user access to the assets by restricting the actions the user can take before being authorised.

5.4.1.3 Help prevent de-activation of other SFRs

The Information Flow Control policy detailed in FDP_IFF.1 along with the other SFRs involved in flow control, provide for rigorous control of allowed data flow, preventing unauthorised deactivation of SFRs.

5.4.2 Justification of Unsupported Dependencies

The SFRs of this Security Target are taken from the CC part 2. Where the SFRs have required dependencies as defined in CC part 2, the supporting SFRs have been included in this ST. There is one family (FMT_MSA) that has been excluded from the Security Target. As a result there are some SFRs included in this ST that will not have their required dependencies met. The FMT_MSA family has been excluded because management of the security attributes is not part of the scope of the TOE. The environmental assumptions A.LOGICAL and A.PHYSICAL state that only trusted agents can access the TOE components where management would be conducted. These environmental constraints suffice in place of the FMT_MSA family.

This Security Target should be read in conjunction with [1] as it defines roles and privileges and access controls regarding the server components of ActivCard's Secure Remote Access.

The requirement FAU_GEN.1 depends on FPT_STM.1 for reliable time stamps. The TOE does not have a clock mechanism and gets the time from the underlying operating system. Security objectives do not specify a *reliable* time stamp is required. However, certain environmental assumptions like A.LOGICAL and A.PHYSICAL are sufficient for the operating system time stamp to be considered appropriate for FAU_GEN.1.

5.4.3 Strength of Functions Claim

This section shows how the minimum strength of function level for the ST is consistent with the security objectives for the TOE. This ST claims SOF-Basic for the strength of functions level of the TOE, as the TOE is used in general commercial systems that may be attacked by intruders with basic attacks. The potential attackers are assumed to have only public knowledge of the TOE, use standard computer equipment, have a proficient knowledge of TCP/IP, no access to server components of the TOE, but may access client application. The strength of function claim of SOF-Basic is suitable to counter this LOW attack rating. Furthermore, the EAL 2 is suitable to provide confidence in the TOE to achieve SOF-Basic and counter LOW rated attacks.

AVA_VLA.1, one of the assurance components from which the EAL2 assurance level is comprised, determines that the "vulnerability analysis is performed by the developer to ascertain the presence of obvious security vulnerabilities, and to confirm that they cannot be exploited in the intended environment for the TOE".

Identification and Authentication provides the basis for access to the client software, smart card, portal and RADIUS authenticator. Authentication to the smart card is required for authentication to other components, thus Strength of Function claims relate to the smart card I&A.

The Smartcard PIN policy is detailed in the TSF CS PIN, section 6.1.1, and details the restrictions on the specification of the smartcard PIN by the user. With this policy in place, the chance of an attacker guessing the correct PIN is reduced. The opportunity to guess the PIN is further limited because the smart card will "Block" after 3 incorrect login attempts. A "Blocked" card requires unblocking by the smart card issuer before the smart card can perform operations.

Based on the information above, a general claim of SoF-Basic is consistent with the security objectives of the TOE, and the policies used to enforce those objectives. A specific claim of SoF-Medium is made for FDP_ACF.1(2) and FIA_UAU.1 (2), which relates directly to the authentication of the user to the smart card.

Evaluation of strength of cryptographic functions is outside the scope of this ST - this relates to the FCS Class of SFR, and to the TSFs IPSec Negotiation, Data Confidentiality, Integrity and Cryptographic Operations.

6 TOE Summary Specification

This section presents the Security Functions implemented by the TOE and the justifications as to why these functions meet the requirements of section 5.

6.1 TOE Security Functions

This section presents the security functions performed by the TOE and provides a mapping between the identified security functions and the Security Functional Requirements that it must satisfy. The functions are described in terms of the TOE. The order of the functions contributes to portraying the sequential order in which the functions are implemented.

6.1.1 Client Software (CS)

The Client software resides on the PC of the end user accessing the SRA service, and provides a GUI for control of the interaction with the Portal and Business. Secure interaction with the Portal and Business are conducted using IPSec (see IPSec component for more detail).

Portal Selection (CS POR)

The Client GUI is started and the user is given the list of Portals to connect with. The portal selection will be used to initiate the connection to the Portal using IPSec. At this point the user has not been positively identified or authenticated (to the portal).

Smart Card authentication (CS S/C)

Certificate is read from smart card after correct PIN is presented (the interaction between smart card and client software is controlled by an access control policy which is enabled upon correct entry of the PIN). Certificate is read once and stored for later use. The PIN input by the user is obscured onscreen by a series of asterisks. At this point the user has not been positively authenticated (to the portal).

RADIUS Authentication (Dial-Up mode only) (CS RAD)

If end-user connects to Portal via modem, then the Client Software dials a RADIUS server. The user name and password presented to the RADIUS server are generated from certain fields of the certificate. The password is an RSA digital signature generated using a hash of the card data. See section 6.1.2.1 for details on how the RADIUS server authenticates the end-user.

Banner presentation (CS BAN)

Once the end-user is authenticated to the Smart Card, the client software does a DNS Look-up to get the Misuse / warning message of the Portal. The Client software displays the banner after receiving it from the Portal. The Client Software has the capability to display further misuse and warning banners for the business gateway to which the client is connecting, if this function has been enabled by the business gateway. The user has to accept the misuse/ warning banner for the user to gain access to the protected network. If the user does not accept the banner then the client application returns to the initial state requiring complete re-authentication.

PIN Changing (CS PIN)

The client software has the ability to alter the PIN used to access the smart card at any time. The smart card is delivered to the client with a pre-loaded PIN which the client is forced to alter at the first use. The existing PIN is required to change to a new PIN.

The client software can be configured to meet an organisational password policy implementing frequency of changes, password length, password complication and number of different passwords before repetition.

On first use of the Client, the user is forced to change the smart card PIN. The new PIN entered is checked against by the PIN policy DLL. The standard policy is summarised here as follows:

1. Minimum length of 6 characters
2. Maximum length of 12 characters
3. Characters permitted: [0-9|A-Z|a-z]
4. Must not contain all the same characters, case insensitive. Example: 111111, aAaAaA
5. Must not be a complete sequence of incremental characters, case insensitive. Example: abcdef or aBcDeF is not acceptable, but 1abcde is acceptable.
6. Must not be a complete sequence of decremental characters, case insensitive. Example: fedcba or FeDcBa is not acceptable, but 1fedcb is.
7. Must not be: ‘welcome’, ‘database’, ‘account’, ‘password’, ‘oracle’, ‘computer’, ‘qwerty’, tyuiop’, ‘asdfgh’, ‘fghjkl’, ‘zxcvbn’ or ‘qwaszx’ of any case combination.
8. Must be different from the OLD PIN.
9. Must not be a complete incremental or decremental number sequence. i.e. the following are not allowed: “0123456”, “567890”, “890123”, “321098”

The customer organisation may specify their own PIN policy, but the above should be used as a minimum baseline.

6.1.2 RADIUS Authentication of end-user (RAD)

Authentication (RAD AUTH)

The RADIUS username/password are obtained from the smart card to prevent them having to be separately managed. The password is a digital signature. The digital signature is created using a hash of the card data, which the card digitally signs. The interaction between the client and the RADIUS authenticator is controlled by an access control policy which specifies the conditions for successful authentication, whereby the RADIUS server looks for the user certificate on an LDAP server, and once found compares the digital signature with the one presented by the client. Any mismatch will result in failure to authenticate.

Anti-replay (RAD ANTI)

RADIUS server keeps a count of how many times each end-user has authenticated via RADIUS. Each time an end-user authenticates the count is incremented. The RADIUS server will deny access attempts (by hanging up) if the presented sequence is less than stored sequence value, providing anti-replay protection.

6.1.3 Portal Authentication of end-user (POR)

The Portal provides authorisation of the users and businesses and assists the establishment of a secure end-to-end connection over an insecure network, using IPSec (see IPSec component for more detail). It can run on a single or multiple machines depending on the capacity required.

LDAP lookup (POR LDAP)

The Portal provides an LDAP interface to the LDAP directory where the user connection permissions are stored. A simple lookup is performed (using TCP) using the user's Distinguished Name (DN). The response is a business-specific DNS identification value, which serves as an index into the DNS.

The client uses the DNS index value to look up the business to which it is connecting on a standard DNS server.

The presence of the user's certificate in the LDAP directory is used to authenticate the user.

Business Locator (Portal mode only) (POR BUS)

Within ESP session the Business Locator lookup is done to provide the client with the Business Gateways information they can access.

The business locator is the primary interface to the services (business) LDAP directory. It understands the schema and stored information that relates to the services and to the users and the relationships between them.

The primary purpose of the business locator is to use this knowledge to answer queries that require this knowledge on the behalf of other network elements.

Active Client Register (POR CLI)

The Portal maintains a register of clients who are connected to the Portal for cross-checking by the Business gateway when the client-business connection is established. The business communicates with the Portal to determine the credentials of the user (See Business Gateway component for more detail). The Business Gateway and Portal establish an IPSec session to protect this communication.

The Active Client Register is used by the gateway to ensure that the user requesting access to the Business Gateway has been verified for access by the Portal. If the user appears in this register, the gateway can establish a trusted IPSec tunnel with that client. If the user does not appear in this list then the user access request is rejected.

6.1.4 IPSec (IP)

The TOE utilises SSH IPSec which conforms to all relevant official and industry standards, including IETF IPSec standards RFC2401 to RFC2412, ISO X.509 v3, RSA Laboratories PKCS-1, PKCS-7, PKCS-10, NIST Digital Signature Standard DSS (FIPS PUB 186), NIST Data Encryption Standard DES (FIPS PUB 46-1) and the ANSI C standard. See Section 9.1.2 for more detail on IPSec negotiation.

IPSec negotiation (IP NEG)

IPSec negotiations are conducted between the client, portal and gateway. IKE (Internet Key Exchange) is used to negotiate a secure tunnel between the entities, called the IKE SA

(Security Association). During this process the two entities authenticate themselves to each other and exchange shared keys (this process involves the generation, distribution and destruction of cryptographic key material). The Diffie-Hellman protocol is used to agree on a common session key, so that the entities can encrypt the IKE tunnel. The exchange is authenticated using PKI. See section 9.1.3 for more detail on Diffie-Hellman.

Data Confidentiality (IP CON)

The TOE implements the IPSec protocol Encapsulated Security Payload (ESP) to provide data integrity, confidentiality and replay detection. Confidentiality is implemented using the 3DES, and AES ciphers. This operation is controlled by an operational policy to prevent the disclosure of data. Table 6-1 provides the encryption algorithms and key sizes implemented.

Integrity (IP INT)

Integrity of transmitted data is implemented using digital signatures based on the SHA-1 standard. Authentication Headers (AH) can also be used to provide data integrity, but ESP provides data encryption as well with minimal overhead (for small amounts of data). This is why the ESP mode is the default mode for SRA. Table 6-1 lists the possible combinations for the hashing and encryption algorithms implemented by SRA.

Main Mode	
SA Hashing algorithm	**SA Encryption algorithm**
SHA-1	3DES
	AES

Table 6-1 IPSec algorithms

6.1.5 Business Gateway (BG)

The ActivCard.com Business Gateway subsystem allows the business to be authenticated by the Portal and to set up a secure end-to-end connection with the ActivCard.com client over an insecure network, using IPSec (see IPSec component for more detail).

Client authentication (BG CLI)

The business gateway verifies with the Portal that a User's access is permitted. To do this the gateway transmits (using UDP) the Distinguished Name (DN) of the User to the Portal, which checks the active users, verifies access for the requesting business and responds with accept or reject. (Also see function POR CLI.) The business gateway can also check CRLs in an LDAP server within the Portal.

6.1.6 Smart Card (SC)

The smart card in conjunction with the PIN identifies the user. The smart card is personalised, and holds public and private keys and the user's X.509 certificate. All signing operations at the client PC are performed on the smart card.

Cryptographic Operations (SC CRY)

The smart card uses 1024 bit RSA cryptography for signing and verification processes. The data to be encrypted is SHA-1 hashed data that has been hashed by the SSH IPSec libraries. The Client software takes the hashed data, adds padding and passes the data to the card to do the encryption.

RSA decryption is performed in software by Client software, which uses the SSH Crypto Library. The certificate is read from the smart card in order to retrieve the public key for this purpose.

Attribute storage (SC ATT)

The smart card maintains security attributes (PIN, X.509 public certificate and private key) within the card memory, for the purposes of identification and authentication of the user. The X.509 certificate is duplicated on the portal LDAP directory.

PIN Blocking (SC PIN)

The smart card is protected by a User-specified PIN, which the user is prompted to enter before card access. If the incorrect PIN is entered three times the smart card will block itself for further PIN-entry attempts.

6.1.7 GW DNS Server (GW)

The Gateway DNS Server can perform load balancing across multiple Gateways using round-robin techniques. It is separate from the Networks standard DNS server.

DNS lookup (GW DNS)

DNS is used to provide the configuration details the client requires such as the IP address of the Gateway and the computer misuse banner screen. This information is used to determine the access allowed between the client and the gateway.

6.1.8 Audit

The RADIUS authenticator, Business Gateway and Portal record events for the audit log. The audit records will be stored in an RDBMS.

The following will be audited with each event:

1. Audit type (SUCCESS or FAILURE);
2. Date/Time (Stored in UTC);
3. Origin (Application, Host, Instance identifier);
4. Event Code
5. Event Parameters

Details will be provided for the meaning of each event and the parameters that apply to each event with each application.

The event parameters will include details on the target of the audit event and any other applicable information for that event type.

The following is an example of the data in an audit event:

1. SUCCESS
2. 2000:06:01 16:08:07

3. ActivCardRemoteGateway / testhost.example.com / UDP:500
4. 45
5. [1/PeerId: C=AU, O=Org, OU=Dev, CN=John Smith], [2/LocalId: C=AU, O=Org, OU=Dev, CN=Gateway023], [3/Initiator: Peer], [4/PeerIP: 10.0.56.123]

In this example we had a *Success*full connection from the IP address *10.0.56.123* by the user with the identity *C=AU, O=Org, OU=Dev, CN=John Smith* to the gateway with the identity *C=AU, O=Org, OU=Dev, CN=Gateway023* and was initiated by the user (not the gateway). The origin indicates that this event was generate by the *ActivCardRemoteGateway* on the host *testhost.example.com* This particular gateway is listening for IKE service on *UDP* port *500*.

Table 6-2 Audit events provides the list of events and descriptions that are recorded.

Event	Description
AUDIT SPECIFIC EVENTS	
Message Table fail	Translation module not loaded.
Interface not found	Translation module interface not found.
Message Table required	No translations found but configuration requires them.
Audit file open fail	Open of audit file failed
Audit file write fail	Write to audit file failed
Audit not open	Audit target is not open
Database connect fail	Failed to connect to database
Database write fail	Failed to write event to database
BUSINESS LOCATOR EVENTS	
Started	Business Locator started
Authorisation success	User authorised success
Authorisation failure	User authorised failure. Reasons being: • User not online at portal • User not subscribed to business • Unknown business • Could not generate business DN • Could not generate user's DN • Could not decode user's DN • User's DN not determined from peer
LDAP events	Failed
	Server online
	Server offline
RADIUS EVENTS	
Startup	Background process failed on startup
Authorisation failures	Request contained no username field
	Username could not be decoded
	Password could not be decoded
	LDAP search for user failed
	No user profile found
	Unsupported authorisation method (Not using digital signatures)
	Password not verified because sent it wrong format
	Failed to access sequence number database

	Failed to update sequence number database
	Sequence number replay
	Digital signature authentication failed
	LDAP: User is suspended
	LDAP: User status contains unknown value
	LDAP: User status contains invalid value
	LDAP: User certificate did not match serial number supplied
Authorisation success	Successful authentication
General	Unsupported attributes in RADIUS request
	Radius encryption method
	Radius Started
Protocol	Client protocol version
	Invalid client protocol
LDAP events	Timeout
	Failed
	No response
GATEWAY EVENTS	
Generic logs	IPSEC WARNING (specific detail entered)
	IPSEC ERROR (specific detail entered)
	IPSEC CRITICAL (specific detail entered)
	IPSEC INFORMATION (specific detail entered)
	IPSEC NOTICE (specific detail entered)
	IPSEC UNKNOWN (specific detail entered)
Authentication events	Authentication success (Phase 1 done)
	Authentication failure (Phase 1 failed)
	Authentication failure (Phase 1) Could not get policy
	Authentication failure (Phase 1) No security policy available
	IP access success (Phase 2 done)
	IP access failure (Phase 2 failed)
Policy events	Manually loaded certificate. Skipping LDAP checks
	PORTAL: could not determine users status
	PORTAL: could not determine service
	PORTAL: user is not online at portal
	PORTAL: user is not subscribed to this business
	PORTAL: portal returned unknown status value
	LDAP validation failed
	Failed to extract certificate from cache
	Failed to extract BER encoding from certificate
	Failed to extract public key from certificate
	Failed to allocate hash for certificate selection
LDAP events	Timeout
	Failed
	No response

Table 6-2 Audit events

6.2 IT Security Functions Rationale

Table 6-3 - TSF vs SFR Mapping

TSF SFR	CS POR	CS S/C	CS RAD	CS BAN	CS PIN	RAD AUTH	RAD ANTI	POR LDAP	POR BUS	POR CLI	IP NEG	IP CON	IP INT	BG CLI	SC CRY	SC ATT	SC PIN	GW DNS	AUDIT
FAU_GEN.1																			✓
FAU_GEN.2																			✓
FAU_SAR.1																			✓
FAU_SAR.2																			✓
FCS_CKM.1											✓								
FCS_CKM.2											✓								
FCS_CKM.4											✓								
FCS_COP.1												✓	✓		✓				
FDP_ACC.1(1)	✓							✓	✓	✓				✓				✓	
FDP_ACC.1(2)		✓			✓														
FDP_ACC.1(3)			✓			✓													
FDP_ACF.1(1)	✓							✓	✓	✓				✓				✓	
FDP_ACF.1(2)		✓			✓														
FDP_ACF.1(3)			✓			✓													
FDP_IFC.2											✓	✓	✓						
FDP_IFF.1											✓	✓	✓						
FDP_ITT.1												✓	✓						
FIA_AFL.1																	✓		
FIA_ATD.1																✓			
FIA_UAU.1(1)	✓							✓			✓								
FIA_UAU.1(2)		✓																	
FIA_UAU.7		✓																	
FIA_UID.1(1)	✓							✓			✓								
FIA_UID.1(2)		✓																	
FPR_ANO.1											✓								
FPT_RPL.1							✓												
FTA_TAB.1				✓															
FTP_ITC.1										✓									

Table 6-4 - TSF Rationale

TOE Component	TSF	SFR

TOE Component	TSF	SFR
Client Software	Portal Selection	Selection of the portal: • Enables the TSF to enforce restrictions on the connection between the protected hosts (FDP_ACC.1(1)); • Restricts the access of clients to portals and gateways based on their IP Address and X.509 certificate (FDP_ACF.1(1)); • Portal selection is allowed before the user has been authenticated (FIA_UAU.1(1)); • Portal selection is allowed before the user has been identified (FIA_UID.1(1)).
	Smart card auth.	The smart card authentication: • Enforces access control restrictions on the access of the client software to the smart card (FDP_ACC.1(2)); • Restricts the access by the client to the smart card based on the PIN presented (FDP_ACF.1(2)); • Requires the correct entry of the PIN before TSF-meditated actions are allowed (FIA_UAU.1(2)); Allows the user to select a Portal to connect to before requiring identification (FIA_UID.1(2)); • Provides limited feedback to the user on presentation of the PIN (FIA_UAU.7);
	RADIUS auth.	The RADIUS authentication: • Enforces access control restrictions on the access of the client software to the portal (FDP_ACC.1(3)); • Restricts the access by the client to the portal according to the digital identity of the client (FDP_ACF.1(3)); • Detects repeated sequence numbers presented by the RADIUS authenticator to protect against replay attacks (FPT_RPL.1).
	Banner pres.	The Banner presentation: • Displays the warning/misuse banner after receiving it from the portal (FTA_TAB.1)
	PIN changing	Changing the smart card PIN: • Permits the enforcement of access control restrictions on the access of the client software to the smart card (FDP_ACC.1(2)); • Permits the enforcement of access control restrictions by the client to the smart card based on the PIN presented (FDP_ACF.1(2)).

TOE Component	TSF	SFR
RADIUS Authentication of end-user	Authentication	RADIUS authentication: • Enforces access control restrictions on the access of the client software to the portal (FDP_ACC.1(3)); Restricts the access by the client to the portal according to the digital identity of the client (FDP_ACF.1(3)).
	Anti-Replay	Anti-replay detection: Detects repeated sequence numbers presented by the RADIUS authenticator to protect against replay attacks (FPT_RPL.1).
Portal Authentication of end-user	LDAP Lookup	LDAP lookup: • Enables the TSF to enforce restrictions on the connection between the protected hosts (FDP_ACC.1(1)); Restricts the access of clients to portals and gateways based on their IP Address and X.509 certificate (FDP_ACF.1(1)); LDAP lookup is allowed before the user has been positively authenticated (FIA_UAU.1(1)); LDAP lookup is allowed before the user has been positively identified (FIA_UID.1(1)).
	Business locator	The business locator: • Enables the TSF to enforce restrictions on the connection between the protected hosts (FDP_ACC.1(1)); Restricts the access of clients to portals and gateways based on their IP Address and X.509 certificate (FDP_ACF.1(1));
	Active Client reg.	The active client register: • Enables the TSF to enforce restrictions on the connection between the protected hosts (FDP_ACC.1(1)); Restricts the access of clients to portals and gateways based on their IP Address and X.509 certificate (FDP_ACF.1(1)); Is used by the TSF to verify the identity of the client, which is necessary for initiation of a secure connection between components (FTP_ITC.1).
IPSec	IPSec negotiation	The IPSec negotiation: • Generates session keys using Diffie-Hellman algorithms (FCS_CKM.1); • Distributes session keys securely between trusted peers using DH protocol (FCS_CKM.2); • Destroy key material after expiry, when security associations are re-negotiated the existing key material is zeroised (FCS_CKM.4);

TOE Component	TSF	SFR
	Data Confidentiality	The TOE provides data confidentiality by: • Utilising proven cryptographic methods for generation of cryptographic key material (FCS_COP.1); • Restricting access between the client and the gateway according to predefined rules, which are enforced according to the IP Address and IPSec parameters of the peers (FDP_IFC.2); • Enforces the information flow control policy to restrict the information flow between client and gateway (FDP_IFF.1); • Enforcing the access control policy and information flow policy to ensure that user data is not disclosed or modified enroute between Client, Portal and Business (FDP_ITT.1).
	Integrity	The TOE provides data integrity by: • Utilising proven cryptographic methods for generation of cryptographic key material (FCS_COP.1); • Restricts access between the client and the gateway according to predefined rules, which are enforced according to the IP Address and IPSec parameters of the peers (FDP_IFC.2) • Enforces the information flow control policy to restrict the information flow between client and gateway (FDP_IFF.1); • Transmissions between Client, Portal and Business are protected from modification and deletion (FDP_ITT.1)
Business Gateway	Client authentication	The client authentication: • Enables the TSF to enforce restrictions on the connection between the protected hosts (FDP_ACC.1(1)); • Restricts the access of clients to portals and gateways based on their IP Address and X.509 certificate (FDP_ACF.1(1));
Smart card	Crypto operations	The smart card performs RSA encryption. The data encrypted is SHA-1 data hashed by the SSH IPSec libraries (FCS_COP.1);
	Attribute storage	The smart card maintains an X.509 certificate, private key and PIN number on the card (FIA_ATD.1)
	PIN Blocking	The card will become blocked and when three unsuccessful attempts are made to enter the correct PIN number (FIA_AFL.1).
GW DNS Server	DNS lookup	The DNS lookup: • Enables the TSF to enforce restrictions on the connection between the protected hosts (FDP_ACC.1(1)); • Restricts the access of clients to portals and gateways

TOE Component	TSF	SFR
		based on their IP Address and X.509 certificate (FDP_ACF.1(1)).
Audit	Audit	The audit functions: • Generate log messages in accordance with FAU_GEN.1; • Associate each audit log event with a user identity (FAU_GEN.2); • Provide the administrator with the ability to review the audit logs (FAU_SAR.1), and restricts all other users access to the logs (FAU_SAR.2);

6.2.1 Strength of Function

Strength of TOE security functions analysis is only performed on probabilistic or permutational functions, except those which are based on cryptography. There are no functions explicitly realised by probabilistic or permutational mechanisms, except for PIN entry, which enables smart card authentication.

TSFs directly related to the authentication of the user to the smart card are Smart Card Authentication (CS S/C) and PIN Changing (CS PIN).

For these security functions, a claim of SoF-Medium is appropriate.

6.2.2 IT Security Function Mutual Support

Whenever a user gains access to a protected resources, they would have been authenticated twice. Once to the smart card to obtain access to their X.509 certificate and secondly to the Portal or RADIUS. Coupled with authentication is the user acceptance of the Misuse / Warning Banner before proceeding. These functions are providing support to each other to verify the user's identity and to allow the IPSec connection to be established using the user's X.509 certificate. Once the IPSec connection is established the user can transmit information across an untrusted network and the information will be protected from disclosure and modification. Therefore, the IT Security Functions are supporting each other to ensure the user's data can be transmitted securely.

The IT Security Functions are the SFRs put into terms of the TOE. So the SFRs mutual support rationale applies to the IT Security Function mutual support rationale. As shown in the above paragraph the extra detail provided in the definition of the IT Security Functions does not undermine the SFR rationale.

7 Security Assurance Requirements and Measures

7.1 Security Assurance Requirements

This Security Target is targeting Evaluation Assurance Level (EAL) 2 package from CC Part 3.

Table 7-1 EAL 2 requirements

Assurance Classes	Assurance Requirements
Configuration Management	ACM_CAP.2
Delivery and Operation	ADO_DEL.1, ADO_IGS.1
Development	ADV_FSP.1 ADV_HLD.1 ADV_RCR.1
Guidance Documents	AGD_ADM.1 AGD_USR.1
Tests	ATE_COV.1 ATE_FUN.1 ATE_IND.2
Vulnerability assessment	AVA_SOF.1 AVA_VLA.1

7.2 Security Assurance Measures

This section describes the assurances measures taken so that SRA satisfies the Security Assurance Requirements for an Evaluation Assurance Level (EAL) 2.

7.2.1 Configuration Management for SRA

The Configuration Management (CM) system used in developing the TOE uniquely identifies the configuration items that compose the TOE. The CM plan lists the configuration items of the TOE and describes how each item is uniquely identified.

The TOE is managed under the Perforce configuration management software.

To ensure customers know they have the correct product, the TOE's documentation, media and software is labelled with a unique version number. The software version can be checked by using the Help | About dialog (or equivalent) on the Client. The software version can be check by using the solaris pkginfo command for the Server components.

7.2.2 SRA Distribution & Delivery Procedures

When distributing or delivering the TOE to users the developers follow the SRA Distribution and Delivery Procedures to ensure that the users get an authentic product.

7.2.3 SRA Development

Documentation generated throughout the development of SRA is:

SRA Functional Specification – a document describing the features and interfaces of the SRA and relevant software.

SRA High Level Design – design documents providing information of the major components that make up the TOE. These documents provide the functionality of each component, emphasising the security functions and the related interfaces.

SRA EAL 2 Correspondence Demonstration – an evaluation specific document showing that TSF representations are complete and consistent throughout the design documentation.

7.2.4 SRA Guidance Documentation

The user guidance is provided by the following Client software documents:

- Remote Access Client Quick Install Guide;
- Remote Access Client Online User Guide.

The administration guidance is provided by the following server documents:

- Remote Access Gateway configuration and administration guide;
- Radiusd configuration and administration guide;
- Business locator configuration and administration guide;
- Remote access modes of operation guide;

7.2.5 SRA Testing

Development of the SRA includes the validation and verification of the product. Test plans and procedures have been developed to prove the functionality of the product as defined in the Functional Specification. Test results have been fed back into the development cycle.

7.2.6 SRA EAL 2 Vulnerability Analysis

An evaluation specific analysis of the TOE will be conducted to show that each claim of strength is exceeded and that all identified vulnerabilities cannot be exploited.

7.3 Security Assurance Requirements Rationale

This section shows that the identified Security Assurance Measures are appropriate to meet the Security Assurance Requirements (SARs) for an EAL 2. Table 7-2 shows the SARs and the corresponding measure to which it is mapped. Also provided is an explanation of how the requirements will be met by the measure.

Table 7-2 - Assurance Measures meet Assurance Requirements

Assurance Requirement	Assurance Measure	How measure meets requirement
ACM_CAP.2	Configuration Management for SRA	Provides all documentation related to the Configuration Management system used in developing the TOE, including information about unique labelling and referencing of the TOE.
ADO_DEL.1	SRA Distribution & Delivery Procedures	Describes the delivery procedures necessary when distributing or delivering the TOE to users.
ADO_IGS.1	The SRA Guidance Documentation	Client software guides describe the necessary steps for secure installation, generation and start-up of the Client software. The administration guides describe the necessary steps for secure installation, generation and start-up of the server component software

Assurance Requirement	Assurance Measure	How measure meets requirement
ADV_FSP.1	SRA Functional Specification	Describes the purpose and method of use of the TSF and external interfaces.
ADV_HLD.1	SRA High Level Design	Presents the structure in terms of sub-systems of the TSF. These sub-systems shall have their security features and structure described and interfaces identified.
ADV_RCR.1	SRA EAL 2 Correspondence Demonstration	This will demonstrate as security functionality is more refined in documentation that no details are missing or inconsistent. This analysis will show mappings from the TOE Summary Specification in ST to the Functional Specification, then from the Functional Specification to the High Level Design.
AGD_ADM.1	The SRA Guidance Documentation - Administration Guides	The Administration Guides are sufficient for the AGD_ADM.1 requirement because they describe the secure installation, maintenance and administration of the server components of the TOE ie not the Client software
AGD_USR.1	The SRA Guidance Documentation - Client software guides	This guide provides user function guidance and warnings about using the TOE.
ATE_COV.1	SRA Test Coverage Analysis	This analysis will show the correspondence between the TSF as described in the Functional Specification and the tests identified in the Test Documentation.
ATE_FUN.1	SRA Test Documentation and Results	Shall contain the test plans, procedures, expected outcomes and actual results
ATE_IND.2	Independent Testing	Resources equivalent to the developer's testing shall be provided to the evaluators so they can conduct independent testing. These resources include the TOE, interfaces and test documentation.
AVA_SOF.1	SRA EAL 2 Vulnerability Analysis	Each claim of strength of security mechanism shall be assessed and shown to exceed that claim.
AVA_VLA.1	SRA EAL 2 Vulnerability Analysis	This analysis will show that all identified vulnerabilities cannot be exploited.

The developers have chosen EAL 2 because it provides a low to moderate level of independently assured security and ensures the TOE is structurally tested. EAL 2 requires the high-level design is independently analysed to provide assurance is the security functions of the token. The developers have determined this level of design information is suitable, sufficient and attainable. EAL 2 also requires independent testing, confirmation of developer testing, strength of function analysis and evidence of a developer search for obvious vulnerabilities. This testing and analyses is sufficient for the TOE to be securely used in its intended environment.

8 Reference Documents

[1] Card Management & Personalisation System Security Target, version 1.2, April 2001.

A Annex A

A.1 IPSec Negotiation

IPSec negotiation in the TOE is divided into two phases.

Internet key exchange (IKE) is used to establish the Phase 1 Security association (SA), using main mode, with the certificate being read from the smart card and the card being used to create and check the digital signatures. The first two messages negotiate the security policy for the exchange. The next two messages perform Diffie-Hellman key exchange and pass nonces to each other. The last two messages are used to authenticate the parties to each other.

The card is used to generate a Signature using the responding nonce and other data. This signature is sent to the Gateway together with the Card Certificate. The Business Gateway does not use the Card Certificate it is sent, but obtains it from a directory look-up.

The Business Gateway validates the Certificate checking its validity date, its CA signature and the CRL. It then uses this certificate to check the signature generated by the card. The main outcome of main mode is matching IKE SAs between peers to provide a protected tunnel for subsequent protected exchanges between the IKE peers.

Phase II negotiation is negotiated using Quick mode. Quick mode occurs after IKE has established the secure tunnel in Phase 1. It negotiates a shared IPSec policy, derives shared secret keying material used for the IPSec security algorithms, and establishes IPSec SAs. When the SA expires (after five hours by default), quick mode exchanges nonces which are used to hash the existing shared secret keys, which refreshes the key material and prevents replay attacks.

A.2 Diffie-Hellman

1. The DH process starts with each peer generating a large prime integer, **p** and **q**. Each peer sends the other its prime integer over the insecure channel. For eg, Peer A sends **p** to Peer B. Each peer then uses the **p** and **q** values to generate **g**, a primitive root of **p**.
2. Each peer generates a private DH key (peer A: X_a, peer B: X_b)
3. Each peer generates a public DH key. The local private key is combined with the prime number **p** and the primitive root **g** in each peer to generate a public key, Y_a for peer A and Y_b for peer B.
4. The public keys Y_a and Y_b are exchanged in public.
5. Each peer generates a shared secret number (ZZ) by combining the public key received from the opposite peer with its own private key.
6. Shared secret keys are derived from the shared secret number ZZ.