CLEARSWIFT™

Deep Secure (CSDS)

Security Target

Document No: DN11240/4

Release Authority: Clearswift

Copyright Notice

Table of Contents

1 Introduction

1.1 ST Identification

Title:	Clearswift Deep Secure (CSDS) Security Target (ST)
Authors:	Ralph Worswick
CC Version:	2.2
ST Version	DN11240/4
General Status:	Approved
TOE	Clearswift Deep Secure (CSDS) Version 2
Keywords:	e-mail content policy enforcement, X.400, SMTP, S/MIME, cryptography, digital signature, encryption, CSDS, Bastion, CSB2, Trusted Solaris, TSOL

This document is the security target for the Common Criteria EAL4 evaluation of Clearswift Deep Secure. It conforms to the Common Criteria for Information Technology Security Evaluation [CC].

1.2 ST Overview

This Security Target defines the security requirements for CSDS, a comprehensive e-mail management software suite supporting simultaneously SMTP and X.400 messaging protocols, including S/MIME signed and encrypted subscriber messages.

The Security Target

- describes CSDS, the assumed environment and the evaluated configurations
- defines the assumptions about the security aspects of the environment in which the CSDS will be used;
- defines the threats that are to be addressed, and organisational security policies that are to be met, by the CSDS;
- defines implementation-independent security objectives of the CSDS and IT environment;
- defines the functional and assurance requirements and measures to meet those objectives; and
- provides rationale for the security objectives, security requirements and measures.

Particular attention is drawn to sections 2.5 and 2.6, which specify the extent of product functionality included in the evaluation.

1.3 CC Conformance Claim

This Security Target is CC Part 2 extended, Part 3 conformant, with a claimed evaluation assurance level of EAL4. It is extended because it contains explicitly stated security functional requirement components.

No conformance with any Protection Profile is claimed.

1.4 Structure of Document

The structure of this document is:

Section 2 Describes the Target of Evaluation (TOE)

Section 3 Defines assumptions about security aspects of the environment, and defines security threats addressed and organisational security policies

Section 4 Defines implementation-independent security objectives for the TOE and the IT environment
Section 5 Defines TOE security functional requirements, security assurance requirements and security requirements for the IT environment
Section 6 Describes CSDS measures to meet the security requirements listed in Section 5
Section 7 Describes the rationale for the security objectives, security requirements and TOE summary specification.

1.5 Commonly Used Terms

The following key terms are used throughout this document:

Abbreviation	Meaning
API	Application Program Interface
CA	Certification Authority
CC	Common Criteria
CrS	Crypto Subsystem
CSB2	Clearswift Bastion 2
CSDS	Clearswift Deep Secure
DAP	Directory Access Protocol
DMZ	De-Militarised Zone
DSA	Directory System Agent
EAL	Evaluation Assurance Level
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
LS	Label Subsystem
LSL	Labelling Support Library
MTA	Message Transfer Agent
PKI	Public Key Infrastructure
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SFL	S/MIME Freeware Library
SOAP	Simple Object Access Protocol
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	Target of Evaluation Security Functions
TSFI	TSF Interface
TSOL	Trusted Solaris
TSP	TOE Security Policy
VIC	Vendor Independent Cryptographic
VICI	Vendor Independent Cryptographic API
VS	Virus Scanner

1.6 Definitions

This section contains definitions of the technical terms that will be used within this document.

Definitions taken from [CSB2_ST] are marked with an asterisk.

Active Message Policy	The Message Policy that is currently loaded into the Policy Engine and defines the CSDS Message Flow Control Policy.
*ARCHIVE compartment**	A type of DMZ compartment that contains the CSB2 trusted archive function.
Authorised administrator	A human user who is known to, identified and authenticated by calls to the IT environment prior to authorised access in one or more assigned roles for the purpose of managing the functions of CSDS or its IT environment.
*Channel**	A sequence of CSB2 compartments comprising, in strict order, the incoming PROXY compartment, zero or one ARCHIVE compartment, between zero and four (inclusive) VET compartments and the outgoing PROXY compartment. Two channels will usually be defined, one for each direction of flow of messages through CSB2, with the incoming PROXY compartment for one channel being the outgoing PROXY compartment for the other channel.
*Compartment**	A distinct area of information in a system, implemented by use of sensitivity labels.
*Compartmented Mode Workstation (CMW)**	A trusted workstation that contains enough built-in security to be able to function as a trusted computer. A CMW is trusted to keep data of different security levels and categories in separate compartments.
*cots role**	A CSB2 configured, TSOL managed, untrusted role which can reconfigure or administer only CSB2 'untrusted' subsystems in PROXY and VET compartments.
CSB2	Any evaluated version of Clearswift CS Bastion 2, also marketed as CS Bastion II, compliant with the SFRs defined in [CSB2_ST].
*CSB2 compartment**	A CMW disjoint compartment used by the CSB2.
*CSB2 IN queue**	A queue which handles subscriber messages entering a DMZ compartment.
*CSB2 OUT queue**	A queue which handles subscriber messages leaving a DMZ compartment in the direction of flow through the channel.
*CSB2 RETURN queue**	A queue which handles subscriber messages leaving a DMZ compartment against the direction of flow through the channel.
CSDS	Two instantiations of Clearswift Deep Secure Policy Server software. CSDS is resident on a single CSB2/TSOL platform, which forms part of the IT environment.

CSDS Administration	The CSDS components that provide the administrative functions required by the authorised CSDS roles.
CSDS Message Policy Administrator	A role that permits an authorised administrator to define and modify the behaviour of a Message Policy.
CSDS Message Policy Selector	A role that permits an authorised administrator to select and activate a Message Policy, and to stop/start a policy engine.
CSDS Queue Manager	A role that permits an authorised administrator to perform message release or message discard actions, and to stop/start a policy engine.
*Disjoint Compartments**	Two compartments that are incomparable in terms of their sensitivity labels (neither compartment dominates the other). Access to one compartment does not imply any access to the other.
*DMZ compartment**	A protected CSB2 compartment reserved for running the CSB2 trusted archive function or additional software to police (e.g. sanction or filter) data flow between subscriber networks.
*DMZ network**	A private, protected network, connected to a DMZ compartment to support DMZ services.
Embedded module	A library, or closely-coupled group of C++ classes, that is physically built and distributed with the TOE but forms part of the IT environment.
External library	A major library that is built and distributed independently of the TOE and forms part of the IT environment. Some external libraries include third party software.
External interface	An interface from the TOE to the IT environment. This includes interfaces to external libraries and embedded modules.
Message	In this document, means a subscriber message.
Message element	An atomic component of a message (or embedded message) derived from the decomposition of all structured formats that CSDS can decompose.
Message Policy	A distinct configuration of the sets of rules that, when loaded into an instantiation of the Policy Engine (i.e. made the active Message Policy), defines the CSDS Message Flow Control Policy. There may be more than one Message Policy stored in a Policy Server and available to the Policy Engine, but only one of these may be active at any one time.
Message transaction	The set of events that occur during an operation performed in accordance with the CSDS Message Flow Control Policy.

Message non-deliver (reject)	The Message Policy initiated event of permanent deletion of a subscriber message from a queue of type IN.
Message discard	The administrator initiated action of authorising permanent deletion of a subscriber message from a queue of type MANUAL.
Message release	The administrator initiated action of authorising movement of a subscriber message from a queue of type MANUAL to a queue of type COMPANY or WORLD.
Policy Engine	The CSDS subsystem that mediates and audits subscriber messages between subscriber networks. CSDS includes two instantiations of the Policy Engine, one for each direction of message flow, each residing in a separate CSB2 channel (comprising two PROXY compartments (with X.400 and/or SMTP proxies) and a single CSB2 DMZ (VET) compartment).
Policy Server	One of two instantiations of the set of CSDS components (including a Policy Engine) required to manage and control subscriber message flow in one direction, each residing in a separate CSB2 channel (comprising two PROXY compartments (with X.400 and/or SMTP proxies) and a single CSB2 DMZ (VET) compartment).
*PROXY compartment**	A CSB2 compartment, which is connected to one of the subscriber networks.
Selected Message Policy	The Message Policy that is currently selected for loading into the Policy Engine when the Policy Engine next re-starts, upon which it becomes the Active Message Policy.
Subscriber	A user that has electronic access to a subscriber network and may submit and receive messages to and from CSDS for delivery to other users on a subscriber network.
Subscriber message	An SMTP or X.400 message (which may include S/MIME signature and/or encryption) received by CSDS from a subscriber for distribution and routing to other subscribers.
Subscriber network	One of two networks (designated Company and World) connected to CSDS such that CSDS mediates all information flows, including subscriber messages, entering and leaving CSDS from and to the networks.
User	A human or IT entity that has an electronic interface with CSDS or its IT environment.
*VET compartment**	A type of DMZ compartment that contains additional software to police (e.g. sanction or filter) data flow between subscriber networks.

1.7 References

[CAPP] Controlled Access Protection Profile, NSA, Version 1.d, 8 October 1999

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004:
Part 1 Introduction and general model, CCIMB-2004-01-001
Part 2 Security functional requirements, CCIMB-2004-01-002
Part 3 Security assurance requirements, CCIMB-2004-01-003

[CSB2_ST] CS Bastion II Security Target (EAL4), Clearswift, DN11272/5, 29/05/03

[LSPP] Labelled Security Protection Profile, Issue 1.b, 8 October 1999

[RBAC] Role Based Access Control Protection Profile, Issue 1.0, 30 July1998.

2 Target of Evaluation (TOE) Description

The scope of the TOE is confined to a subset of the CSDS product. Sections 2.1 to 2.4 describe product features and usage considerations of relevance to the TOE. This gives a context to the TOE specification given by sections 2.5 and 2.6. Section 2.7 adds further information on the evaluated configuration.

2.1 Overview

Clearswift Deep Secure (CSDS) is a comprehensive e-mail management software suite supporting simultaneously SMTP and X.400 messaging protocols, including S/MIME signed and encrypted subscriber messages.

The purpose of CSDS is to provide controlled and audited flow of subscriber messages passing between two subscriber networks. CSDS mediates the flow of a subscriber message in accordance with a specific entry in the current organisational security policy (active Message Policy), which is determined from attributes of the subscriber message, including its originator and recipients.

CSDS supports a number of administrative roles that permit authorised administrators to define and modify Message Policy, select and activate a specific Message Policy, manage message queues and stop/re-start the Policy Engine.

Each instance of CSDS operates independently of any other instance of CSDS, although any number of instances of CSDS may be co-located and jointly managed. CSDS may be managed entirely from the DMZ network, or partially remotely from another network connected to the DMZ network (see Section 2.2 for further detail).

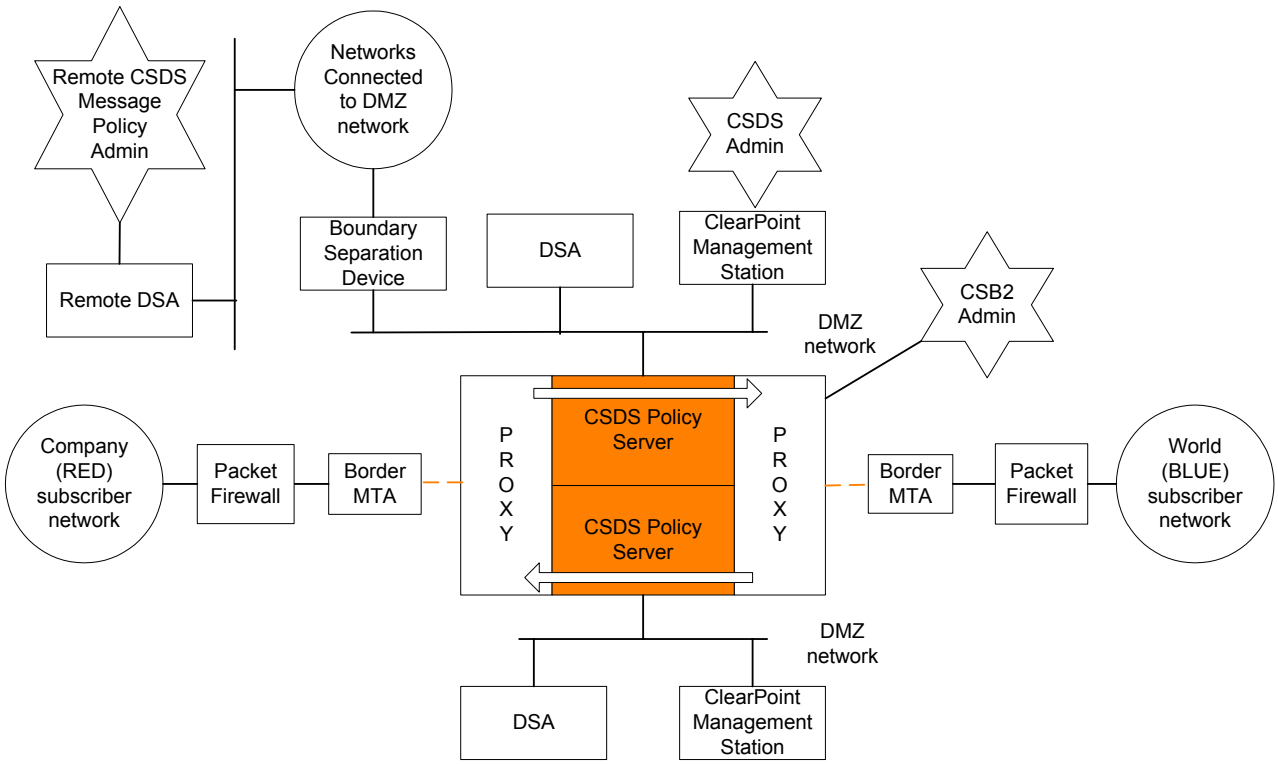
CSDS resides on and interfaces with a single EAL4 certified CSB2/TSOL platform, which provides CSDS with two channels, one for each direction of message flow between the two subscriber networks, and assured separation between channels. Each CSB2 channel consists of two PROXY compartments (with X.400 and/or SMTP proxies) and a single CSB2 DMZ (VET) compartment. The CSB2/TSOL platform also provides assured separation between each CSB2 DMZ (VET) compartment and each of the two CSB2 PROXY compartments, containing the SMTP or X.400 proxies, one for each subscriber network. The CSB2/TSOL platform forms part of the local IT environment of CSDS (see Section 2.3 for further detail).

CSDS comprises two Policy Servers, one for each direction of message flow between the two subscriber networks, each residing in the CSB2 VET compartment associated with the direction of message flow (see Section 2.4 for further detail).

2.2 IT Environment

A single instance of CSDS is connected to two subscriber networks. One network is designated the ‘Company’ network (generally the network that is part of the organisation that controls CSDS); the other network is designated the ‘World’ network. The Company network is labelled RED; the World network is labelled BLUE. Connection is via the PROXY compartments of the CSB2/TSOL platform (see Figure 2.1).

It is assumed that a packet firewall is used to protect CSDS and the CSB2/TSOL platform from denial of service attacks from each subscriber network. A border MTA would normally be used to concentrate subscriber message traffic.



Single CSDS (coloured area = two instances of Policy Server)
Also illustrates location of administrators (remote shown for only one Policy Server)

Figure 2.1 Single CSDS in its assumed environment

As stated in Section 2.1, CSDS comprises two Policy Servers, one for each direction of message flow between the two subscriber networks. Each Policy Server resides in a separate CSB2 DMZ (VET) compartment and must be connected to a separate DMZ network. Each DMZ network must contain a ClearPoint Management Station for management of the associated Policy Server. Selection and activation of a specific Message Policy, management of message queues and stop/re-start of the Policy Engine must be performed using the ClearPoint Management Station on the DMZ network; definition and modification of Message Policy may be performed using the ClearPoint Management Station on the DMZ network or remotely from another network connected to the DMZ network.

Each Policy Server may optionally be configured for exclusively remote definition and modification of Message Policy. This is assumed to be achieved via synchronisation with one DSA on the DMZ network, which is itself synchronised with a remote DSA, which holds the Message Policy. It is further assumed that the DMZ network, including CSDS and the CSB2/TSOL platform, is protected from attacks from connected networks containing the remote

DSA by an appropriately assured boundary separation device (e.g. a packet firewall and application level firewall). Appropriate assurance for the boundary separation device would depend on the nature of the connected networks, and in the extreme case where the networks were connected to one or other of the subscriber networks this boundary separation device must provide at least the level of protection provided by CSB2 to its DMZ, and the appropriate assurance level would be EAL4/E3. Protection is assumed to be provided against unauthorised access attempts, including attempts to select or activate a specific Message Policy or manage message queues or stop/re-start the Policy Engine, message modification or eavesdropping attacks, and denial of service attacks.

As stated in Section 2.1, each instance of CSDS operates independently of any other instance of CSDS, although any number of instances of CSDS may be co-located and jointly managed. Co-located and jointly managed instances of CSDS are referred to as a CSDS Policy Server farm (see Figures 2.2a and 2.2b for two example configurations). In a CSDS Policy Server farm it is assumed that each of the Policy Servers on different instances of CSDS that are controlling message flow in the same direction (i.e. from Company to World, or from World to Company) do not share the same DMZ network as the Policy Servers controlling message flow in the other direction.

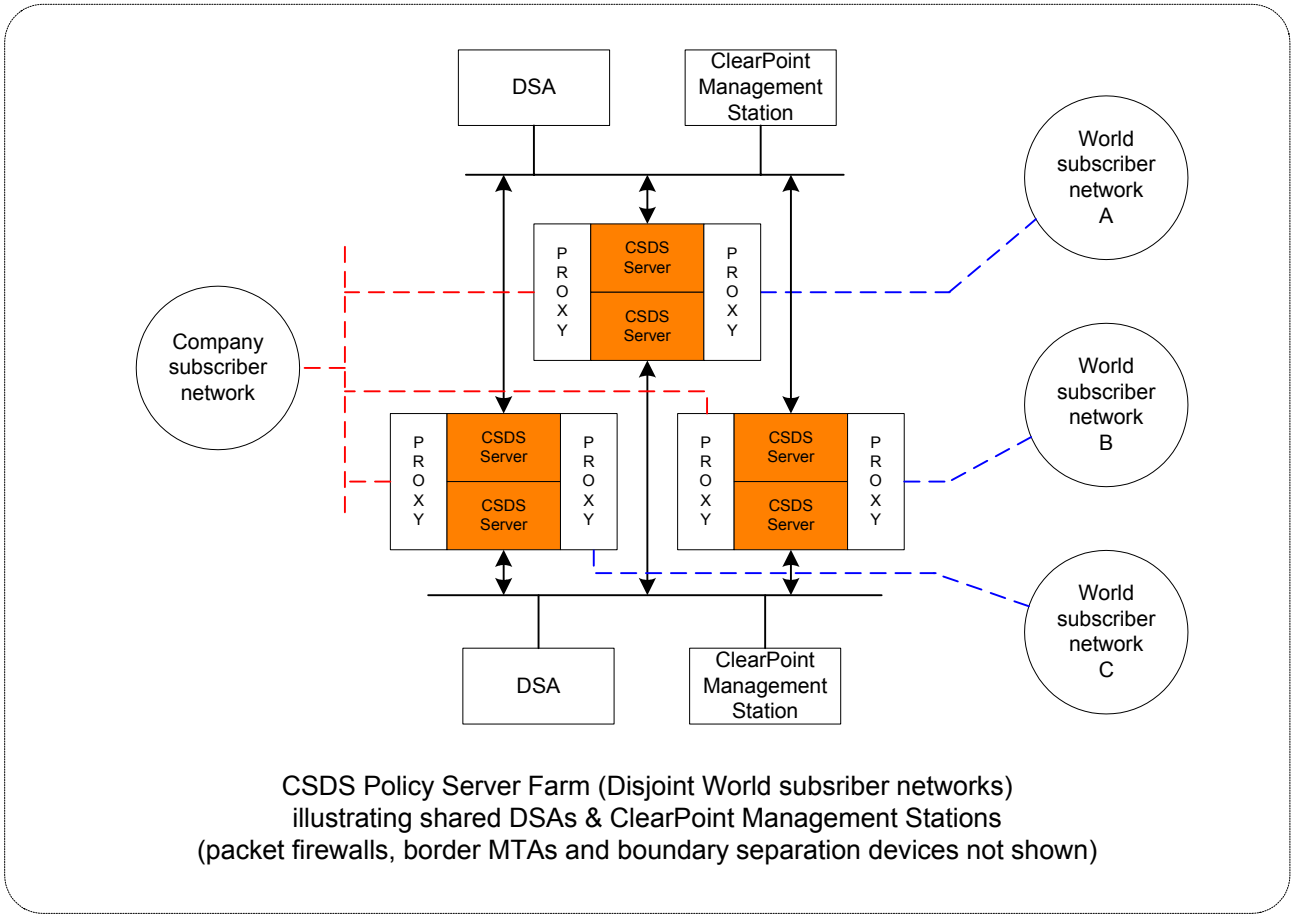


Figure 2.2a CSDS Policy Server Farm (Example 1)

It is assumed that management of the CSB2/TSOL platform is achieved via direct local access to the platform, and not via the DMZ network.

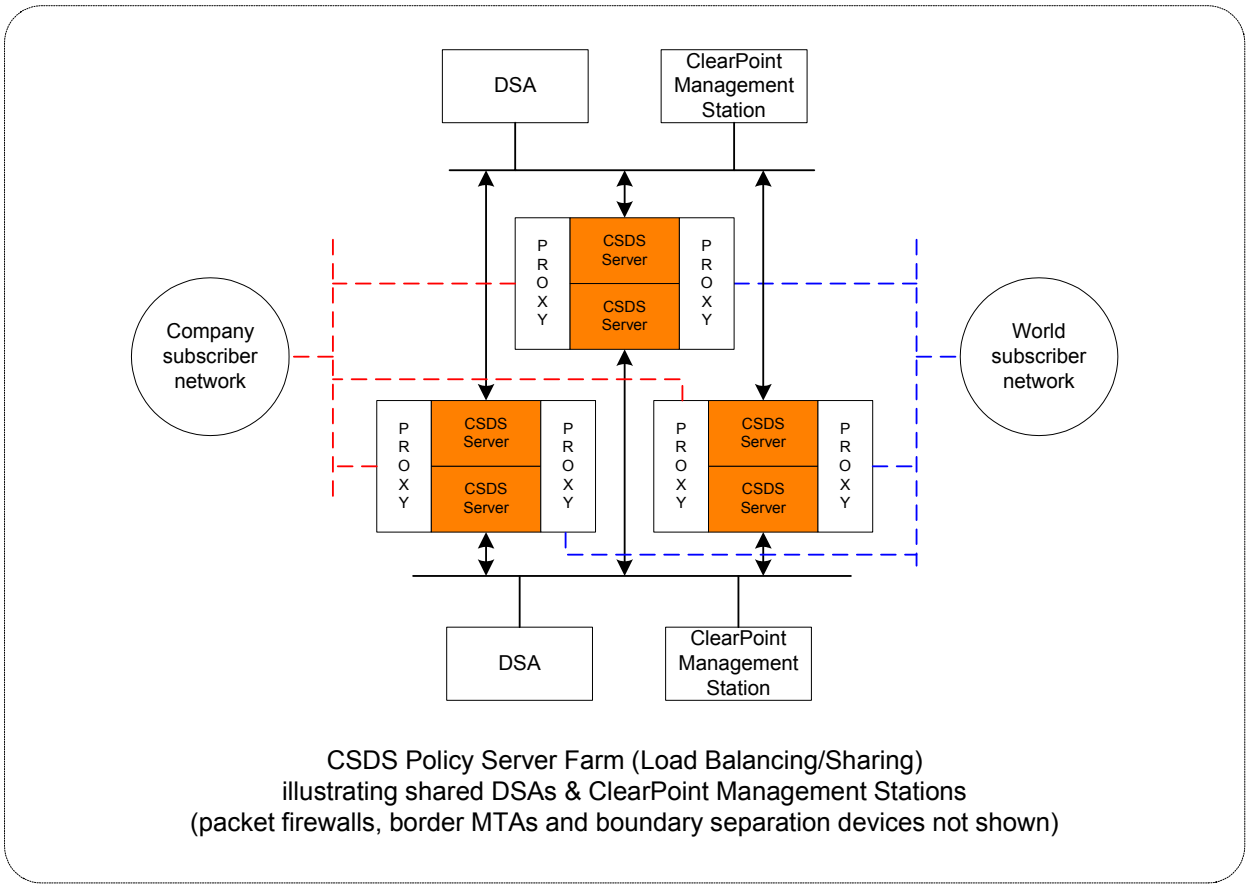


Figure 2.2b CSDS Policy Server Farm (Example 2)

2.3 CSB2/TSOL Platform

The CSB2/TSOL platform forms part of the local IT environment of CSDS.

As stated in Section 2.1, CSDS resides on and interfaces with a single EAL4 certified CSB2/TSOL platform, which provides CSDS with two channels, one for each direction of message flow between the two subscriber networks, and assured separation between channels. Each CSB2 channel consists of two PROXY compartments (with X.400 and/or SMTP proxies) and a single CSB2 DMZ (VET) compartment. The configuration of CSB2 required for CSDS is achieved during the installation of CSDS and is one of the evaluated configurations of CSB2 (see [CSB2_ST]). The CSB2 optional DMZ (ARCHIVE) compartment is not used in CSDS – CSDS message archiving is performed directly by the Policy Server in the VET compartment.

The CSB2/TSOL platform also provides assured separation between the two CSB2 PROXY compartments, containing the SMTP or X.400 proxies, one for each subscriber network. Again, the configuration of CSB2 PROXY compartments, NICs and their connection to the correct

Company and World networks, and the connection of DMZ networks to the appropriate DMZ (VET) compartments and associated NICs, is achieved during the installation of CSDS.

Assured separation between channels and compartments is achieved by the CSB2 utilisation of TSOL Mandatory Access Control (MAC) features. CSB2 also makes use of the other standard security features of TSOL provided in accordance with its role as a trusted operating system compliant with the [CC] protection profiles [LSPP] and [RBAC]. For example, CSB2 uses TSOL Discretionary Access Control (DAC) and Role Based Access Control (RBAC) features to provide CSB2 administrative roles. In addition to the provision of TSOL and CSB2 administrative roles required to manage the CSB2/TSOL platform, CSDS also relies directly on an appropriate CSB2 administrative role for the installation and management of CSDS cryptographic keys and root certificates.

2.4 CSDS

As stated in Section 2.1, CSDS comprises two Policy Servers, one for each direction of message flow between the two subscriber networks, each residing in the CSB2 VET compartment associated with the direction of message flow.

A Policy Server comprises the following services:

- Policy Engine
- CSDS Administration
- Queue Manager.

The Policy Engine is responsible for mediating and auditing the flow of subscriber messages between subscriber networks, and for the application of appropriate import and export controls, in accordance with the active Message Policy. Message security labels may be extracted in accordance with a proprietary standard, with RFC 2634 or with STANAG 4406. Encrypted messages are decrypted in order to perform the required mediation, and then re-encrypted if required. Decrypted messages are protected from unauthorised access by the CSB2/TSOL platform assured separation and role mechanisms.

Message Policy consists of sets of policy attribute settings between pairs of objects, where objects are in a hierarchy with either Company network or World network as the root and structured as Domains, Groups and Users (Subscribers) below the root. The principle of "management by exception" is implemented, whereby generic policy settings at one level of the hierarchy are inherited by lower levels, unless an explicit exception policy is set at the lower levels.

Each Policy Server may contain any number of Message Policies, which are part of CSDS. One of the Message Policies may be selected for loading into the Policy Engine when it is next re-started. The Message Policy currently loaded into the Policy Engine is referred to as the active Message Policy.

Mediation of a message consists of selecting the appropriate policy attribute settings corresponding to the subscriber message originator/recipient pair, performing the appropriate checks, reviewing and performing the resulting actions.

Checks that may be performed by the Policy Engine include:
- File-type
- Maximum message size
- Valid Security Label
- Clearance dominates the Security Label
- Specified filtering checks (e.g. lexical scanning and virus scanning)
- PKI state (which invokes cryptographic functions).

Actions that may be performed by the Policy Engine include:
- Archive message, inbound or outbound
- Audit message transaction
- Release message
- Hold message for manual intervention by CSDS Queue Manager
- Non-deliver (delete) message
- Remove or replace message parts
- Send notification messages or non-delivery reports.

The following external libraries are used by CSDS and form part of the IT environment:
- Crypto subsystem, which is assumed to work correctly and securely
- Label subsystem, which is assumed to work correctly and securely
- VS filters, which are assumed to scan message elements in order to detect malicious code corresponding to a set of malicious code definitions.

CSDS ensures that cryptographic and label checking operations are handled correctly by invoking the crypto subsystem and label subsystem via a vendor independent cryptographic API (VICI). The crypto subsystem communicates with a DSA on the DMZ network via DAP or LDAP to access, for example, public keys, certificates and certificate revocation lists.

Incoming messages enter the Policy Engine via its IN queue and successfully mediated messages leave the Policy Engine via its COMPANY or WORLD queue (depending on the recipient's domain association with the Company or the World network). Messages that fail mediation may be non-delivered or placed in a MANUAL queue (to be held for examination, action and possible deletion or release by the CSDS Queue Manager administrator role).

The Queue Manager service is responsible for the association of Policy Engine queues with CSB2 queues in accordance with the direction of message flow through the Policy Server. The Policy Engine IN queue is always associated with the CSB2 IN queue.

If the direction of message flow is from the Company network to the World network, then messages destined for the World network leave via the Policy Engine WORLD queue, which is associated with the CSB2 OUT queue, and messages destined for the Company network leave via the Policy Engine COMPANY queue, which is associated with the CSB2 RETURN queue.

If the direction of message flow is from the World network to the Company network, then messages destined for the Company network leave via the Policy Engine COMPANY queue, which is associated with the CSB2 OUT queue, and messages destined for the World network leave via the Policy Engine WORLD queue, which is associated with the CSB2 RETURN queue.

CSDS Administration supports administration of the Message Policy and Policy Engine queues by authorised CSDS administrators acting in the following roles:

- CSDS Message Policy Administrator, who is permitted to define and modify the behaviour of a Message Policy
- CSDS Message Policy Selector, who is permitted to select and activate a Message Policy and to stop/re-start a Policy Engine
- CSDS Queue Manager, who is permitted to perform message release or message discard actions on subscriber messages in MANUAL queues, and to stop/re-start a Policy Engine.

CSDS administrators are identified and authenticated using X.509 certificates via the cryptographic functions invoked through VICI.

As described in Section 2.2, selection and activation of a Message Policy and a stop/re-start of a Policy Engine (by a CSDS Message Policy Selector), message release and discard actions and a stop/re-start of a Policy Engine (by a CSDS Queue Manager) must be performed using the ClearPoint Management Station on the DMZ network. Definition and modification of a Message Policy (by a CSDS Message Policy Administrator) may be performed using the ClearPoint Management Station on the DMZ network connecting to the policy server, or remotely from another network connected to the DMZ network via a remote ClearPoint Management Station connecting to a remote DSA that stores the master copy of the Message Policy and replicates this Message Policy to a DSA on the DMZ network- however, it is assumed that the IT environment is configured so that this administration is exclusively from the DMZ network, or exclusively remote.

Communication between CSDS Administration and the local ClearPoint Management Station is via the SOAP/XML protocols over HTTP over SSL (Implemented by OpenSSL with calls to VICI). Communication between the CSDS Administration and a DSA is through VICI and via DAP or LDAP.

The integrity of each Message Policy transferred from a remote DSA to a DSA on the DMZ network is protected by a digital signature, which is applied by the remote ClearPoint Management Station and verified by the crypto subsystem provided by the IT environment.

CSDS Administration records the following audit events:

- Authentication attempts
- Changes to a Message Policy
- Access exceptions.

Audit trail data generated by the Policy Engine and CSDS Administration is stamped with a dependable date and time when recorded.

The major components and data flows within CSDS are illustrated in Figure 2.3. The Queue Manager component is not shown, but the various queues are.

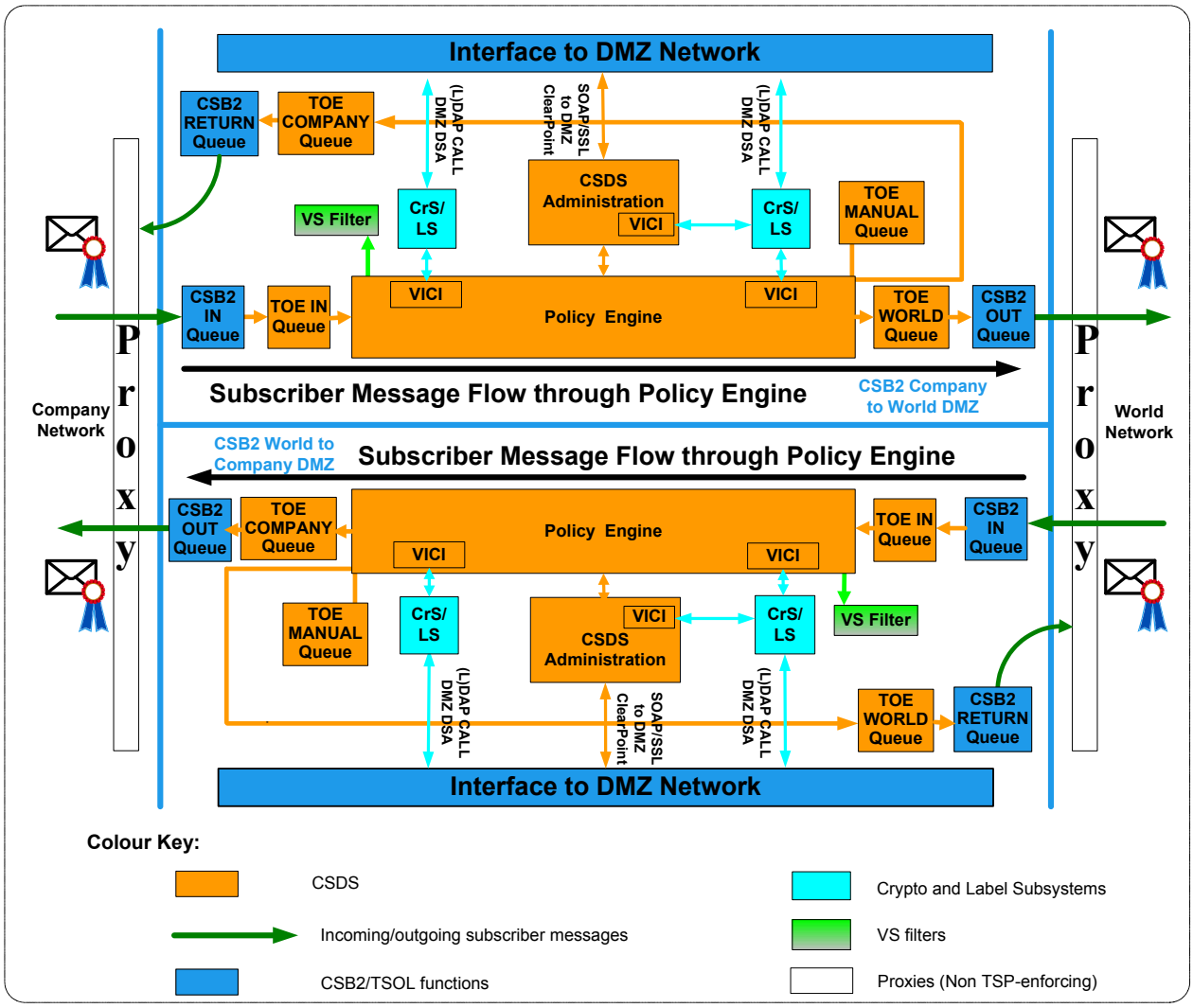


Figure 2.3 CSDS

2.5 Logical TOE Description

The TOE comprises the following aspects of CSDS message-flow management functionality:

- Accurate identification and validation of all originator/recipient pairings (relationships) per message. A valid pairing must fall within the domains defined by, and controlled by, current active message-flow policy.
- Invocation of all necessary message-flow mediation checks (on the message elements derived from preliminary message unpacking) in accordance with per-relationship policy requirements. The checks result in zero or more policy event triggers.
- Correct application of cryptographic operations, security label checking operations and virus scanning. For these functions the TOE boundary extends to the correct handling of calls to the underlying external libraries, which provide the basic functions on which these policy operations depend.
- Release, deletion or queuing for manual inspection of messages as required by policy event triggers.

- Invocation of excluded supplementary message handling actions (below) as required by policy event triggers.
- Release or deletion of messages in accordance with manual inspection directives.
- Logging of associated audit records.
- Accurate routing and delivery of released messages, including internally generated notifications, to the correct subscriber network interface.
- Separation, on the CSDS policy server, of the management roles defined for manipulation of message queues and message-flow policies.
- Application, on the CSDS policy server, of the TOE security management functions (updating, selecting, activating Message Policy, managing messages in queues and stopping/starting a policy engine).

CSDS functionality thus excluded from the TOE includes:

- Correct unpacking of messages into message elements, and reassembly of message elements into output messages.
- The mediation checks applied to message elements (some of which use external libraries).
- Actions to remove, replace or annotate message content, as required by policy event triggers.
- Actions to generate notification messages, as required by policy event triggers.
- Actions to generate inbound or outbound archives, as required by policy event triggers.
- The management interface running on ClearPoint Management Stations.

2.6 Physical TOE Description

Physically the TOE comprises those software components of a CSDS Policy Server which provide the logical functionality specified in the above section, specifically:

- The Policy Engine, except the exclusions identified in the next paragraph.
- The CSDS Administration process (including a DSA synchronisation agent), excluding the Cryptographic Subsystem.
- The Queue Manager.

The TOE excludes the following software components, which form the TOE IT environment:

- The CSDS Policy Engine embedded modules that implement:
    - Message decomposition and re-composition functions;
    - policy mediation check functions (as listed as excluded in section 2.5); and
    - policy action functions (as listed as excluded in section 2.5).
- The CSDS Policy Engine external libraries for:
    - virus scanning (VS filters);
    - cryptography (Cryptographic Subsystem); and
    - formal security labels (Label Subsystem).

- The encompassing system environment:
    - CSB2 and TSOL8 for CSDS Server.
- ClearPoint Management Stations.
- X.500 Directory Servers (DSAs).
- Certification Authority software to create X.509 Certificates and Certificate Revocation Lists.
- The CSDS Directory Synchronisation Agent for uploading virus definition updates into a remote X.500 Directory Server.
- Border MTAs.
- Boundary Separation devices.

Note that the embedded modules and external libraries listed above (first two major bullets) are bound with the TOE at run-time, and thus share some memory and stack. No architectural separation mechanisms exist to enforce non-interference, but a degree of protection is provided by object orientated encapsulation principles that are employed consistently at all interfaces to ensure TOE data structures are protected as private or read-only data[1].

On the interface with the local ClearPoint: Message Policy can be modified by ClearPoint and loaded onto the Policy Server; and commands can select active policy, stop/start Policy Engine, inspect Manual queues and individual messages in these and release or discard these messages, etc. All these interactions are conveyed by authenticated SSL, and the Policy Server uses VICI to validate the administrator's identity.

On the interface with the DSA, Message Policies each with an associated attribute integrity information attribute (digital signature) are downloaded from the DSA to the Policy Server. VICI is used to validate the integrity of each Message Policy, and to authenticate the CSDS Message Policy Administrator who modified it. No data can be uploaded from the Policy Server to the DSA. The Policy Server initiates all connections, and provides authentication to the DSA if required.

2.7 Evaluated Configuration

The target of the evaluation (TOE) is the specified subset of CSDS (Policy Server) software:

- Clearswift Deep Secure Release 2.0 E2 Pkg Vn 2.02.37.

In the following configurations:

- Configured with remote distribution of Message Policy & VS virus definition updates disabled
- Configured with remote distribution of Message Policy & VS virus definition updates enabled
- Configured with between zero and two VSs enabled.

Executing on the following items of software and hardware which form part of the TOE environment:

[1] References to TOE data-structures are in general not passed across external interfaces, but where this does occur read and write access is via call-back into the TOE.

- A single SUN SPARC Workstation that supports SUN Trusted Solaris
- An evaluated version of SUN Trusted Solaris, compliant with the [LSPP] and [RBAC] protection profiles, in its evaluated configuration
- An evaluated version of CSB2, compliant with the SFRs defined in [CSB2_ST], in its evaluated configuration with two channels, each channel containing two PROXY compartments (with X.400 and/or SMTP proxies), one DMZ (VET) compartment and zero DMZ (ARCHIVE) compartments.

Also including in the TOE environment one instance of a VIC crypto subsystem[2], the following specific VIC crypto subsystems having been selected for inclusion in the evaluated test configuration:
- 'Cryptomathic PrimeInk Premium VIC for CSDS' Pkg Vn 1.0.07
- 'SFL VIC for CSDS' Pkg Vn 3.0.36
- 'Null VIC for CSDS' Pkg Vn 3.0.36

Also including in the TOE environment one instance of an LSL label subsystem[3], the following specific LSL label subsystems having been selected for inclusion in the evaluated test configuration:
- 'X.841 LSL for CSDS' Pkg Vn 3.0.36
- 'Null LSL for CSDS' Pkg Vn 3.0.36

Also including in the TOE environment between zero and four optional VS filters[4], the following specific VS filters having been selected for inclusion in the evaluated test configuration:
- Sophos SAVI VS Issues Jan 2003, June 2003 & September 2003
- CSAV command AV for Solaris Vn 4.70.0

And TOE environment DSA and network configurations[5]:
- Null VIC for CSDS and Null LSL for CSDS with no DSA
- SFL VIC for CSDS and Null LSL for CSDS configured with LDAP access to DSA
- SFL VIC for CSDS and X.841 LSL for CSDS configured with DAP access to DSA
- SFL VIC for CSDS and X.841 LSL for CSDS configured with LDAP access to DSA
- Cryptomathic PrimeInk Premium VIC for CSDS and X.841 LSL for CSDS configured with DAP access to DSA
- Operating in an environment that may contain any number of other instances of the TOE, where the DMZ networks for a given direction of subscriber message flow are connected as a CSDS Policy Server farm (see Figures 2.2a and 2.2b)
- Message Policy definition and modification by the CSDS Message Policy Administrator via a separate ClearPoint Management Station attached to each separate DMZ network

---

[2] A rationale for alternative VIC crypto subsystems is presented in Annex A
[3] A rationale for alternative LSL label subsystems is presented in Annex B
[4] A rational for alternative VS filters is presented in Annex C
[5] Developer testing is organised such that each VS filter is tested with each combination of VIC crypto subsystem and LSL label subsystem.

- Message Policy definition and modification by the CSDS Message Policy Administrator via synchronisation with a separate DSA attached to each separate DMZ network, where the CSDS Message Policy Administrator is accessing a remote DSA from the remote location, which is then synchronised with the DSA on the DMZ network via a DMZ connection that is protected in accordance with A.DMZ_Protection and A.Remote_Admin.

Note that management of the TOE by a CSDS Message Policy Selector and a CSDS Queue Manager is always enabled via a separate ClearPoint Management Station attached to each separate DMZ network.

3 TOE Security Environment

3.1 Secure Usage Assumptions

A.Access_to_Passwords: Authorised administrator access to passwords
Cryptographic keys and root certificates must be protected so that authorised administrators can neither access nor modify them outside of authorised TOE IT Environment functions.

A.Admin_Docs: Documentation for authorised administrators
Authorised administrators must follow the policies and procedures defined in the TOE documentation for secure administration of the TOE.

A.Competent_Admin: Competent authorised administrators
Authorised administrators must be competent to manage the TOE and the security of the information it contains.

A.No_Abuse_By_Admin: No abuse of authority by authorised administrators
Authorised administrators must be trusted not to abuse their authority.

A.Prot_Against_Nature: Natural disaster protection
The system must be adequately protected against natural disasters such as fires and floods (e.g., sprinkler systems, alarms, etc.).

A.Prot_Agnst_Pwr_Fail: Power failure protection
The system must have adequate backup power sources to ensure that sudden losses of power do not affect availability of service or loss of data.

A.Platform_Admin: Platform administration
Administration of the CSB2 and TSOL platform must be performed locally and not via a DMZ network.

A.Policy_Admin: Policy administration
Authorised administrators acting in the role of a CSDS Message Policy Administrator shall perform the role either exclusively locally via the DMZ network or exclusively remotely.

A.Remote_Admin: Remote administration
CSDS Message Policy Administrators outside the DMZ network shall only be able to define and modify Message Policy settings, and only via networks connected to the DMZ network.

A.Remote_Admin_Env: Remote administration environment
Authorised administrators outside the DMZ network shall operate in a controlled and well-managed environment which restricts definition and modification of Message Policy to authorised CSDS Message Policy Administrators and affords an equivalent level of protection as that required for the DMZ network environment.

A.Remote_Message_Policy: Remote Message Policy Integrity
The integrity of Message Policies transferred from a remote DSA to a DSA on the DMZ network must be protected by digital signatures, which are verified by the crypto subsystem provided by the IT environment.

A.Review_Audit_Log: Authorised administrators review audit logs
Authorised administrators shall review audit logs regularly.

A.DMZ_Protection: Adequate protection of the DMZ
The DMZ network must be protected. The DMZ network must be protected from any other connected network by an appropriately assured (up to EAL4/E3) and configured boundary separation device.

A.DMZ_Separation: Separation of the DMZ for each direction of flow
DMZ network(s) connected to one or more Policy Servers on different instances of CSDS that are controlling message flow in the same direction (i.e. from Company to World, or from World to Company) must not share the same DMZ network(s) as the Policy Servers controlling message flow in the other direction.

A.DOS_Protection: Protection against Denial of Service
The CSDS must be protected against Denial of Service attacks. This might be by a border MTA protected by a packet firewall.

A.Crypto_Keys: Crypto Key Management
Authorised administrators shall enter, maintain and delete cryptographic keys in a secure manner.

3.2 Threats to Security

T.Admin_UserPriv: Administrator violates user privacy policy
An authorised administrator learns the identity (or other privacy related information) of user(s) in violation of subscriber privacy policy. Privacy-related information is sensitive information associated with the identity of a user.

T.Hack_AC: Systems fails to detect hacker access
A hacker gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability.

T.Hack_Avl_Resource: Hacker attempts resource denial of service
A hacker executes commands, sends data, or performs other operations that make system resources unavailable to system users. Resources that may be denied to users include bandwidth, processor time, memory, and data storage.

T.Hack_Masq: Hacker masquerades as legitimate user or system process
A hacker masquerades as a subscriber or administrator to perform operations that will be attributed to the subscriber or administrator or a system process.

T.Inapprop_Rel_Info: **Inappropriate release of information**
Unauthorised release of information from the DMZ into a subscriber network.

3.3 Organisational Security Policies

P.Accountability: **Individual accountability**
Individuals shall be held accountable for their actions.

P.Authorized_Use: **Authorised use of information**
Information shall be used only for its authorised purpose(s).

P.Marking: **Information marking**
Information shall be appropriately marked with an appropriate label.

P.Physical_Control: **Physical protection**
Information shall be physically protected to prevent unauthorised disclosure, destruction, or modification.

P.Crypto: **Cryptographic Protection**
Cryptographic operations shall be performed in a secure manner. This shall include entering and deleting of cryptographic keys.

P.Info_Flow_Control: **Control of Information Flow**
Information shall be protected to prevent unauthorised flow of information.

P.Anti_Virus: **Virus Scanner Filters**
It shall be possible to scan subscriber message elements for malicious code corresponding to a set of malicious code definitions.

4 Security Objectives

4.1 Security Objectives for the TOE

O.Accountability: Accountability of Information Flows
The TOE must provide subscriber accountability of information flows through the TOE and for authorised administrator use of security related functions.

O.Audit_Records: Record Readable Audit Trail
The TOE must provide a means to record an audit trail of security related events, with accurate dates and times.

O.Controlled_Flow: Controlled Information Flow
Information cannot flow through the TOE between two subscriber networks unless it passes through the Policy Engine.

O.IDAuth: Unique Identity and Authentication
The TOE must uniquely identify and authenticate the claimed identity of all TOE authorised administrators before granting them access to TOE functions. The TOE must protect the authenticity of any Message Policy change made by an authorised administrator.

O.SecFun: Secure Administration Functions
The TOE must provide functionality that enables authorised administrators to manage the TOE security functions.

O.Mediat: Mediation of Flow of Information
The TOE must mediate the flow of all information between connected subscriber networks governed by the TOE, in accordance with the Message Policy, ensuring that checks and actions are invoked in accordance with specific security attributes of each subscriber message. However, the enforcement of the checks and actions is excluded from the scope of the evaluation.

O.Crypto: Cryptographic Operations
The TOE must ensure that cryptographic operations are correctly handled.

O.Anti_Virus: Virus Scanner Filters
The TOE must enable scanning of subscriber message elements for malicious code as required by the Message Policy.

4.2 Security Objectives for the Environment

OE.ConFlo: Controlled Information Flow
Information cannot flow between subscriber networks unless it passes through the Policy Engine.

OE.IDAuth: Unique Identity and Authentication
The IT environment must uniquely identify and authenticate the claimed identity of all

authorised administrators of the IT environment before granting them access to IT environment functions.

OE.Admin: Well Behaved Administrator
Those responsible for administering the TOE and the IT environment must be competent and trustworthy in order to manage the security functions effectively. Effective management is necessary in order that the threats are not inadvertently or deliberately realized.

OE.Admin_Docs: Documentation for authorised administrators
Authorised administrators must follow the policies and procedures defined in the TOE documentation for secure administration of the TOE.

OE.NoRemo: No Remote Access
Subscribers and authorised administrators cannot directly access the TOE or the IT environment from the internal or external subscriber networks.

OE.SecFun: Secure Administration Functions
The IT environment must provide functionality that enables authorised administrators of the IT environment to manage the IT environment security functions.

OE.Access_to_Passwords: Authorised administrator access to passwords
Cryptographic keys and root certificates must be protected so that authorised administrators can neither access nor modify them outside of authorised TOE IT Environment functions.

OE.SecSta: Secure Startup of Service
Upon initial start up of the TOE or recovery from an interruption in TOE service, the IT environment must not compromise its resources or those of any connected network.

OE.Prot_Against_Nature: Natural disaster protection
The system must be adequately protected against natural disasters such as fires and floods (e.g., sprinkler systems, alarms, etc.).

OE.Prot_Agnst_Pwr_Fail: Power failure protection
The system must have adequate backup power sources to ensure that sudden losses of power do not affect availability of service or loss of data.

OE.Platform_Admin: Platform administration
Administration of the CSB2 and TSOL platform must be performed locally and not via a DMZ network.

OE.Policy_Admin: Policy administration
Authorised administrators acting in the role of a CSDS Message Policy Administrator shall perform the role either exclusively locally via the DMZ network or exclusively remotely.

OE.Remote_Admin: Remote administration
CSDS Message Policy Administrators outside the DMZ network shall only be able to define and modify Message Policy settings, and only via networks connected to the DMZ network.

OE.Remote_Admin_Env: Remote administration environment
Authorised administrators outside the DMZ network shall operate in a controlled and well-managed environment which restricts definition and modification of Message Policy to authorised CSDS Message Policy Administrators and affords an equivalent level of protection as that required for the DMZ network environment.

OE.Remote_Message_Policy: Remote Message Policy Integrity
The integrity of Message Policies transferred from a remote DSA to a DSA on the DMZ network must be protected by digital signatures, which are verified by the crypto subsystem provided by the IT environment.

OE.Review_Audit_Log: Authorised administrators review audit logs
Authorised administrators shall review audit logs regularly.

OE.Residual_info: No Residual Information
The IT environment must ensure that residual information from a previous information flow is not transmitted in any way and is unavailable for reuse.

OE.DMZ_Protection: Adequate Protection of the DMZ
The DMZ network must be protected. The DMZ network must be protected from any other connected network by an appropriately assured (up to EAL4/E3) and configured boundary separation device.

OE.DMZ_Separation: Separation of the DMZ for each direction of flow
DMZ network(s) connected to one or more Policy Servers on different instances of CSDS that are controlling message flow in the same direction (i.e. from Company to World, or from World to Company) must not share the same DMZ network(s) as the Policy Servers controlling message flow in the other direction.

OE.DOS_Protection: Protection against Denial of Service
The environment of the CSDS must provide protection against Denial of Service attacks.

OE.Physical_Control: Physical Protection of the CSDS
The CSDS must be located in a physical environment that physically protects it against unauthorised access to information stored or in transit through the CSDS.

OE.Crypto_Ops: Cryptographic Operations
The IT environment must provide correct and secure cryptographic functions for use by the TOE.

OE.Crypto_Keys: Crypto Key Management
Authorised administrators of the IT environment shall enter, maintain and delete cryptographic keys in a secure manner.

OE.Label_Check: Label Checking Operations
The IT environment must provide correct and secure label checking functions for use by the TOE, which check that a given label is valid and dominated by a specified clearance.

OE.Accountability: Individual Accountability
The IT environment must ensure that authorised administrators of the IT environment are held accountable for their actions.

OE.Auditing: Audit Recording & Reporting
The IT environment must record the security relevant actions of users of the IT environment, with accurate dates and times. The IT environment must present this information to authorized administrators.

OE.Anti_Virus: Virus Scanner Filters
The IT environment must provide Virus Scanner (VS) filters for use by the TOE which scan message elements for malicious code corresponding to a set of malicious code definitions.

5 IT Security Requirements

Functional requirements are specified below (sections 5.1 & 5.3) in respect of functionality provided by the TOE and external libraries. In accordance with the TOE specification given by sections 2.5 and 2.6, some CSDS product functionality is excluded from the TOE and thus forms part of the IT environment for the TOE. IT environment requirements (section 5.3) are not specified in respect of this functionality, but are implied.

5.1 TOE Security Functional Requirements

5.1.1 Introduction

The following functional components are taken directly from CC Part 2, except those marked as '(explicitly stated)'. Tailored requirements are defined with assignments, selections and refinements underlined. Where there is a reference to 'users' this must be interpreted as authorised administrators of the TOE rather than subscribers, unless otherwise stated.

5.1.2 Security Audit (FAU)

5.1.2.1 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) Changes to the Message Policy;
c) Authentication attempts[6];
d) Access exceptions;
e) Message transactions. 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, the additional information specified in Table 5.1. FAU_GEN.1.2

Table 5.1 Additional Information in Auditable Events

Section	Component	Event	Additional Information
5.1.2.1	FAU_GEN.1	Start-up and shutdown of the audit functions.	
5.1.2.2	FAU_GEN.2	None.	
5.1.3.1	FCS_COP.1X	None.	
5.1.4.1	FDP_IFC.1	None.	
5.1.4.2	FDP_IFF.1	Message transactions.	Message identifiers, message subject, message recipients, message security label (if present).

[6] Application Note: Each transaction is individually authenticated, hence there is no concept of 'log on' or 'log off'.

Section	Component	Event	Additional Information
5.1.4.3	FDP_LCK.1X	None.	
5.1.5.1	FIA_UAU.2X	Authentication attempts[7].	Identification of the specific Policy Server (Policy Server ID) on which authentication was performed. If failed – the reason If successful – the granted access control level.
5.1.5.2	FIA_UID.2X	Authentication attempts.	Identification of the specific Policy Server (Policy Server ID) on which authentication was performed. If failed – the reason If successful – the granted access control level.
5.1.6.1	FMC_VSF.1X	None	
5.1.7.1	FMT_MSA.1	Access exceptions.	Reason for failure.
5.1.7.2	FMT_MSA.3X	None	
5.1.7.3	FMT_SMF.1	Changes to the Message Policy.	Message Policy identity.
5.1.7.4	FMT_SMR.1	None.	

5.1.2.2 User identity association (FAU_GEN.2)

The TSF shall be able to associate each auditable event with the identity of the user[8] that caused the event. FAU_GEN.2.1

Additional dependency: FDP_IFF.1

5.1.3 Cryptographic support (FCS)

5.1.3.1 Calls to cryptographic operations (FCS_COP.1X) (explicitly stated)

Hierarchical to: No other components.

The TSF shall perform properly formed calls to symmetric and asymmetric encryption and digital signature operations in accordance with, as a minimum: FCS_COP.1X.1

a) RSA

[7] Application Note: A single audit event is logged for each identification and authentication attempt – the operations specified by FIA_UID.2X and FIA_UAU.2X are implemented in a single combined function.

[8] Application Note: In this case, user means subscriber or authorised administrator. In the case of an event caused by a subscriber, the subscriber identity is not established by FIA_UID.1, but by FDP_IFF.1, and may be represented by the subscriber email address or Distinguished Name depending on the security attributes associated with the message.

b) DSA
c) Diffie-Hellman
d) Triple DES
that meet recognised standards.

Dependencies: FCS_COP.1 Cryptographic operation.

5.1.4 User data protection (FDP)

5.1.4.1 Subset information flow control (FDP_IFC.1)

The TSF shall enforce the CSDS Message Flow Control Policy on: FDP_IFC.1.1

a) Subjects: Policy Engine and CSDS Administration
b) Information: subscriber messages
c) Operations: the movement of a subscriber message from a queue of type IN to a queue of type WORLD or COMPANY; the movement of a subscriber message from a queue of type IN to a queue of type MANUAL; the non-delivery (permanent deletion) of a message from a queue of type IN; the discard (permanent deletion) of a message from type MANUAL; the movement of a subscriber message from a queue of type MANUAL to a queue of type WORLD or COMPANY.

5.1.4.2 Simple security attributes (FDP_IFF.1)

The TSF shall enforce the CSDS Message Flow Control Policy[9] based on the following types of subject and information security attributes: FDP_IFF.1.1

a) Subject security attributes:
    i) The Policy Engine's active Message Policy
    ii) The CSDS Administration's Message Policies
    iii) The CSDS Administration's selected Message Policy
b) Information security attributes:
    i) The message's queue type[10]: IN, WORLD, COMPANY, MANUAL
    ii) The message's sender identity (email address and/or Distinguished Name)
    iii) The message's recipient identity (email address)
    iv) The message's PKI state: plain; signed; encrypted (usually as part of a triple wrap); or any arbitrary combination of these
    v) The message's associated certificates
    vi) The message's security label[11]
    vii) The message's message elements and their respective file type
    viii) The message's size.

[9] Application Note: The CSDS Message Flow Control Policy is wider in scope than the Message Policy.
[10] Application Note: The message's queue type is the type of message queue holding the message at the start or end of an operation.
[11] Application Note: The message security label may be a label extracted from the message in accordance with: a proprietary standard (from the Subject field or the first line of message text); RFC 2634; or STANAG 4406.

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: FDP_IFF.1.2

a) The Policy Engine shall move a message from a message queue of type IN to a message queue of type WORLD or COMPANY if all of the active Message Policy conditions configured for the message's sender/recipient pair are met[12], which shall include zero or more of the following:
    i) The sender and recipient are authorised subscribers
    ii) The message is signed
    iii) If signed, the signatures and associated certificates are authenticated
    iv) The message is encrypted
    v) If encrypted, the message and all embedded encrypted messages can be decrypted
    vi) All message elements are authorised file types
    vii) All message elements pass specified filtering checks, e.g. virus scanning; lexical scanning
    viii) The message size is within the configured maximum message size
    ix) The message contains a valid security label[11]
    x) The clearance[13] dominates the security label[11]
b) The Policy Engine shall be permitted to move a message from a message queue of type IN to a message queue of type MANUAL provided one or more of the active Message Policy conditions configured for the message's sender/recipient pair are not met, which shall include zero or more of the conditions listed in FDP_IFF.1.2a.
c) The Policy Engine shall be permitted to non-deliver (permanently delete) a message from a message queue of type IN provided one or more of the active Message Policy conditions configured for the message's sender/recipient pair are not met, which shall include zero or more of the conditions listed in FDP_IFF.1.2a.

The TSF shall enforce the following additional rules:

a) If configured in the active Message Policy for the message's sender/recipient pair[14]: FDP_IFF.1.3
    i) The Policy Engine shall direct that a message element is removed or replaced by Message Policy configured text before being moved
    ii) The Policy Engine shall direct that a copy of the subscriber message is placed in an archive in queue prior to the enforcement of the Message Policy, and/or placed in an archive out queue subsequent to the enforcement of the Message Policy
    iii) The Policy Engine shall direct that a non-delivery report is sent to the sender via the WORLD or COMPANY queue
    iv) The Policy Engine shall direct that a notification message is sent to the sender via the WORLD or COMPANY queue, if a security violation occurs

[12] Application Note: In all cases except item i), where the active Message Policy requires a check to be made, the TSF ensures that an appropriate interface is invoked to enforce the check, but the TSF excludes the correct operation of the check.

[13] Application Note: The clearance is an attribute of the Message Policy for the message's sender/recipient pair.

[14] Application Note: In all cases, where the TSF directs that an action be performed, the TSF excludes the action that is performed.

v) The Policy Engine shall direct that an information message is sent to the sender, recipient, and/or an authorised administrator, via the WORLD and/or COMPANY queue, if a subscriber message is being held in the MANUAL queue.

b) The Policy Engine shall ensure that the PKI state of any subscriber message moved to a message queue of type WORLD or COMPANY is one of:
   i) Plain
   ii) Signed
   iii) Triple wrapped.

The TSF shall provide the following: FDP_IFF.1.4

a) Configuration of CSB2 to utilise two active CSB2 channels (each comprising a single VET compartment and two PROXY compartments), one for each direction of subscriber message flow through CSDS
b) A separate instantiation of the Policy Engine in each CSB2 VET compartment
c) An association[15] between CSB2 VET IN, OUT and RETURN queues and the corresponding Policy Engine IN, WORLD and COMPANY queues[16]
d) A Policy Engine MANUAL[17] queue in the same CSB2 VET compartment.

The TSF shall explicitly authorise an information flow based on the following rules: FDP_IFF.1.5

a) An authorised administrator, acting in the role of CSDS Queue Manager, shall be permitted to authorise the movement of a subscriber message from a message queue of type MANUAL to a message queue of type WORLD or COMPANY (thus releasing a message that was held in the MANUAL queue).
b) An authorised administrator, acting in the role of CSDS Queue Manager, shall be permitted to authorise the discard (permanent deletion) of a subscriber message from a message queue of type MANUAL.

The TSF shall explicitly deny an information flow based on the following rules: none. FDP_IFF.1.6

5.1.4.3 Calls to label checking operations (FDP_LCK.1X) (explicitly stated)

Hierarchical to: No other components.

The TSF shall perform properly formed calls to message security label validity and clearance checking operations. FDP_LCK.1X.1

---

[15] Application Note: The meaning of association here is that a specific message in a CSB2 queue of one type is equivalent to the same message in a CSDS queue of an equivalent type corresponding to the direction of message flow (the queue may be identical, or there is a CSDS TSF function that moves the message between corresponding queues (in the same CSB2 DMZ compartment).

[16] Application Note: If the direction of message flow is from COMPANY to WORLD, then OUT corresponds to WORLD and RETURN corresponds to COMPANY. If the direction of message flow is from WORLD to COMPANY, then OUT corresponds to COMPANY and RETURN corresponds to WORLD. CSB2 IN always corresponds to CSDS IN.

[17] Application Note: The CSDS MANUAL queue does not correspond with the CSB2 REJECT queue, which is not used in CSDS.

Dependencies: FDP_LCK.2X Label checking operations.

5.1.5 Identification and authentication (FIA)

5.1.5.1 User authentication before any action (FIA_UAU.2X) (explicitly stated)

Hierarchical to: No other components.

The TSF shall require each user to be successfully authenticated[18] by appropriate calls to cryptographic operations before allowing any other TSF-mediated actions on behalf of that user. FIA_UAU.2X.1

Dependencies: FCS_COP.1X Calls to cryptographic operations.

5.1.5.2 User identification before any action (FIA_UID.2X) (explicitly stated)

Hierarchical to: FIA_UID.1.

The TSF shall require each user to identify itself[19] by appropriate calls to cryptographic operations before allowing any other TSF-mediated actions on behalf of that user. FIA_UID.2X.1

Dependencies: FCS_COP.1X Calls to cryptographic operations.

5.1.6 Malicious Code Handling (FMC) (Extended Class)

5.1.6.1 Calls to Virus Scanner Filters (FMC_VSF.1X) (explicitly stated)

Hierarchical to: No other components.

The TSF shall perform properly formed calls to Virus Scanner Filters. FMC_VSF.1X.1

Dependencies: FMC_VSF.2X Virus Scanner Filters.

5.1.7 Security management (FMT)[20]

5.1.7.1 Management of security attributes (FMT_MSA.1)

The TSF shall enforce the CSDS Message Flow Control Policy to restrict the ability to manage the security attributes in the following list to the authorised roles identified in the following list: FMT_MSA.1.1

a) An authorised administrator acting in the role of CSDS Message Policy Administrator shall be permitted to define and modify the behaviour of a Message Policy

[18] Application Note: Authentication is performed by the cryptographic operations.
[19] Application Note: Identification is performed by the cryptographic operations.
[20] Application Note: There is no default CSDS Message Flow Control Policy, as CSDS is installed and configured initially with no available Message Policy. In this state, the Policy Engine will not operate and all message flow will effectively be disabled. Thus FMT_MSA.3 is not appropriate.

b) An authorised administrator acting in the role of CSDS Message Policy Selector shall be permitted to select and activate a Message Policy and to stop/re-start a Policy Engine

c) An authorised administrator, acting in the role of CSDS Queue Manager, shall be permitted to stop/re-start a Policy Engine and to authorise message release or message discard actions.

5.1.7.2 Static attribute initialisation (FMT_MSA.3X) (explicitly stated)

Hierarchical to: No other components.

The TSF shall enforce the CSDS Message Flow Control Policy to ensure that no subscriber message flow is permitted prior to the selection and activation of a Message Policy. FMT_MSA.3X.1

Dependencies: FMT_MSA.1 Management of security attributes.

5.1.7.3 Specification of Management Functions (FMT_SMF.1)

The TSF shall be capable of performing the following security management functions: FMT_SMF.1.1

a) Define and modify the behaviour of a Message Policy[21]
b) Select a Message Policy
c) Activate a Message Policy[22]
d) Manage Policy Engine queues
e) Stop/re-start a Policy Engine.

5.1.7.4 Security roles (FMT_SMR.1)

The TSF shall maintain the roles[23]: FMT_SMR.1.1

a) CSDS Queue Manager,
b) CSDS Message Policy Selector,
c) CSDS Message Policy Administrator.

The TSF shall be able to associate users with roles. FMT_SMR.1.2

---

[21] Application Note: Message Policy consists of sets of policy attribute settings between pairs of objects, where objects are in a hierarchy with either Company network or World network as the root and structured as Domains, Groups and Users (Subscribers) below the root. The principle of "management by exception" is implemented, whereby generic policy settings at one level of the hierarchy are inherited by lower levels, unless an explicit exception policy is set at the lower levels.

[22] Application Note: When a change is made remotely by a CSDS Message Policy Administrator to a Message Policy, if that Message Policy is the active Message Policy, once it is downloaded to the Policy Server, the CSDS Administration service will force a re-start of the Policy Engine, thus updating the loaded (active) Message Policy. When a change is made locally to an active Message Policy, the change will only be loaded into the Policy Engine by an explicit action of a CSDS Message Policy Selector, or when the Policy Engine is re-started.

[23] Application Note: The CSDS roles defined here do not correspond with the CSB2 roles; however, they operate in a single CSB2 VET compartment and do effectively inherit the privileges of a CSB2 cots role.

5.1.8 Strength of Function Claim

There are no mechanisms in the TOE for which a Strength Of Function claim must be made.

The TOE relies on mechanisms provided in the TOE environment.

Cryptographic functions are provided by a dedicated library. The evaluation of the implementation of the algorithms is outside the scope of this evaluation.

5.2 TOE Security Assurance Requirements

The TOE shall meet the assurance requirements of [CC] Part 3 EAL4 with no augmentation or extension.

5.3 Security Requirements for the IT Environment

5.3.1 Introduction

In order to operate in a secure manner the CSDS relies on CSB2, which in turn relies on TSOL to provide some protection.

Specifically, CSDS relies on the following CSB2 SFRs, which are described in the CSB2 Security Target [CSB2_ST] Section 5.1:

a) FAU_GEN.4 Audit data generation
b) FDP_IFC.1 Subset information flow control
c) FDP_IFF.1 Simple security attributes
d) FMT_MOF.1 Management of security functions behaviour
e) FMT_SMR.4 Security roles.

CSDS relies on all of the TSOL SFRs that are required to comply with [LSPP] and [RBAC] protection profiles.

CSDS also relies on a number of external libraries, as follows:

a) A selected crypto subsystem to perform cryptographic operations and associated key management, the security requirements for which are described in Section 5.3.2
b) A selected label subsystem to perform label checking operations, the security requirements for which are described in Section 5.3.3
c) Between zero and four optional VS filters to scan subscriber message elements to identify malicious code, the security requirements for which are described in Section 5.3.4.

CSDS also relies on the use of the crypto subsystem digital signature operations to verify the integrity of Message Policies received from a remote DSA (via a DSA on the DMZ network), the security requirements for which are described in Section 5.3.5.

CSDS also relies on:

a) Security functions implemented on hardware separate from the CSB2/TSOL platform that protect CSDS and the CSB2/TSOL platform from denial of service attacks (OE.DOS_Protection) originating from the subscriber networks

b) Where other networks are connected to a DMZ network, security functions appropriately assured (up to EAL4/E3), implemented on hardware separate from the CSB2/TSOL platform that protect CSDS and the CSB2/TSOL platform from:
   i) denial of service attacks (OE.DOS_Protection) originating from networks attached to a DMZ network
   ii) unauthorised access from networks attached to a DMZ network (OE.DMZ_Protection)
   iii) any attempted changes to CSDS by remote CSDS administrators from networks attached to a DMZ network, except for changes to Message Policy settings instigated by CSDS Message Policy Administrators (OE.Remote_Admin).

In order to provide the security functions described in the previous paragraph, required to protect CSDS and the CSB2/TSOL platform from specific attacks originating from the subscriber networks and networks attached to a DMZ network, as a minimum the following SFRs are required to be implemented by the IT Environment:

a) FAU_GEN.1
b) FAU_SAR.1
c) FDP_IFC.1
d) FDP_IFF.1
e) FIA_UAU.1
f) FIA_UID.1
g) FMT_MSA.1
h) FMT_MSA.3
i) FMT_SMF.1
j) FMT_SMR.1
k) FPT_STM.1.

Finally the TOE relies on other CSDS product software, specified above in sections 2.5 and 2.6. A number of environmental SFRs are implied in respect of this. The nature of the functionality involved is such that many of these would be 'explicitly stated' rather than taken directly from CC Part 2.

5.3.2 Cryptographic support (FCS)

5.3.2.1 Cryptographic Key Generation (FCS_CKM.1)[24]

The IT environment shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Triple DES and specified cryptographic key sizes at least 112 bits that meet the following: RFC-2630 and ANSI X9.52. FCS_CKM.1.1

[24] Application Note: The IT Environment may be extended to include other key generation algorithms in accordance with other key sizes and standards.

5.3.2.2 Cryptographic key distribution (FCS_CKM.2)[25]

The IT environment shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method key agreement using Diffie-Hellman that meets the following: RFC-2630 and RFC-2631. FCS_CKM.2.1;1

The IT environment shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method key transport using RSA that meets the following: RFC-2630, RFC-3447 and RFC-3560. FCS_CKM.2.1;2

The IT environment shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method symmetric key-encryprion key using Triple DES that meets the following: RFC-2630 and ANSI X9.52. FCS_CKM.2.1;3

5.3.2.3 Cryptographic key destruction (FCS_CKM.4)

The IT environment shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method object reuse that meets the following: [LSPP]. FCS_CKM.4.1

5.3.2.4 Cryptographic Operations (FCS_COP.1)[26]

The IT environment shall perform asymmetric encryption and digital signature operations in accordance with a specified cryptographic algorithm RSA and cryptographic key sizes of at least 1024 bits that meet the following: RFC-3447. FCS_COP.1.1;1

The IT environment shall perform digital signature operations in accordance with a specified cryptographic algorithm DSA and cryptographic key sizes of at least 1024 bits that meet the following: FIPS Pub 186. FCS_COP.1.1;2

The IT environment shall perform asymmetric encryption in accordance with a specified cryptographic algorithm Diffie-Hellman and cryptographic key sizes of at least 1024 bits that meet the following: RFC-2630. FCS_COP.1.1;3

The IT environment shall perform symmetric encryption in accordance with a specified cryptographic algorithm Triple DES and cryptographic key sizes of at least 112 bits that meet the following: ANSI X9.52. FCS_COP.1.1;4

5.3.3 Label checking operations (FDP_LCK.2X) (explicitly stated)[27]

Hierarchical to: No other components.

The IT environment shall check the validity of a given message security label and check that the label is dominated by a specified clearance. FDP_LCK.2X.1

---

[25] Application Note: The IT Environment may be extended to include other key distribution methods in accordance with other standards.

[26] Application Note: The IT Environment may be extended to include other cryptographic operations in accordance with other algorithms, key sizes and standards.

[27] Application Note: The IT Environment may be extended to include label checking operations performed in accordance with standards which specify the checks required.

Dependencies: No dependencies.

5.3.4 Malicious Code Handling (FMC) (Extended Class)

5.3.4.1 Virus Scanner Filters (FMC_VSF.2X) (explicitly stated)

Hierarchical to: No other components.

The IT environment shall scan message elements in order to detect malicious code corresponding to a set of malicious code definitions. FMC_VSF.2X.1

Dependencies: No dependencies.

5.3.5 Inter-TSF detection of modification (FPT_ITI.1)

The IT environment shall provide the capability to detect modification of all IT environment data during transmission from a remote trusted IT product to the TSF within the following metric: data integrity assurance shall be provided in accordance with selected digital signature operations. FPT_ITI.1.1

The IT environment shall provide the capability to verify the integrity of all IT environment data transmitted from a remote trusted IT product to the TSF and perform transmission operation failure and notification if modifications are detected. FPT_ITI.1.2

Dependencies: FCS_COP.1 Cryptographic Operations

6 TOE Summary Specification

6.1 TOE Security Functions

6.1.1 Message Policy Functions

POL-1: Subscriber messages may arrive from a subscriber network in one of the following states:

a) Neither signed nor encrypted;

b) Signed but not encrypted;

c) Triple wrapped (signed, encrypted and then signed again);

d) With any arbitrary nesting of signed and encrypted, such as:

i) Signed and encrypted; or

ii) Just encrypted.

Subscriber messages may leave the CSDS in one of the following states:

a) Neither signed nor encrypted;

b) Signed but not encrypted;

c) Triple wrapped.

POL-2: Prior to selection and activation of a Message Policy, the TOE shall ensure that no subscriber message flow is permitted. An active Message Policy shall be applied by the TOE to all subscriber messages. This Message Policy shall permit policy settings that:[28]

a) Control which subscribers can release messages from one network to another:

i) hold or reject (non-deliver), with or without a non-delivery notification, messages originated by unauthorised subscribers

ii) hold or reject, with or without a non-delivery report, messages addressed to unauthorised subscribers.

b) Hold or reject any unsigned messages.

c) Hold or reject any digitally signed messages that fail authentication.

d) Hold or reject any unencrypted messages.

e) Hold or reject any encrypted messages, or messages containing embedded encrypted messages that cannot be decrypted.

f) Hold or reject messages containing message elements that are not within a configurable set of allowable file-types.

[28] In accordance with section 2.5, the TOE ensures that checks and actions are invoked, but excludes performance of the checks and supplementary actions.

g) Hold or reject all messages containing message elements that fail specified filtering checks, e.g. virus scanning; lexical scanning

h) Hold or reject all messages over a configurable size

i) Hold or reject any message transiting through the TOE if the message does not contain a valid security label[29]

j) Hold or reject any message transiting through the TOE to a destination unless the clearance dominates the message security label[29]

k) Direct that a message element is removed or replaced by Message Policy configured text

l) Direct that incoming and/or outgoing messages are archived

m) Direct that originators are notified regarding security violations at the CSDS

n) Direct that originators are sent a report regarding message non-delivery if a message is rejected

o) Direct that an originator, or recipient, or administrator (or any combination) is advised of a message being held

p) Direct that messages are digitally signed

q) Direct that messages are triple wrapped.

6.1.2 Certificates

CERT-1: There shall be an interface to cryptographic functions that validate certificate paths for messages originating using appropriate trust points.

Note that any limit on the length of the certificate path shall be configured into the Basic Constraints element of the CA Certificate by the CA.

6.1.3 Auditing

AUD-1: As a minimum the CSDS shall log the following events:

a) Authentication attempts;
b) Start-up and shutdown of CSDS audit functions and associated details;
c) Changes to the Message Policy;
d) Access exceptions; and
e) Message transactions.

[29] Application Note: The message security label may be a label extracted from the message in accordance with: a proprietary standard (from the Subject field or the first line of message text); RFC 2634; or STANAG 4406.

AUD-2: The CSDS log shall record for each event:

a) Date;
b) Time;
c) Type of event;
d) Subject identity (the sender email address and/or Distinguished Name in the case of message transactions and security policy exceptions; the Policy Server ID in the case of start-up and shutdown of audit functions; the user ID supplied in the case of authentication attempts, access exceptions and changes to the Message Policy);
e) Success or failure of the attempt;
f) Additional information for specific events, as specified in Table 5.1.

6.1.4 Identification and Authentication

I&A-1: All users of the TOE (i.e. CSDS, not user of TSOL or CSB2, which are authenticated locally by TSOL) shall successfully complete an identification and authentication process before any interaction with the TOE is possible. This will be achieved using individual authenticated certificates.

6.1.5 Access Control

AC-1: The TOE shall restrict access to TOE facilities to users acting in specific roles, as follows:

a) A CSDS Message Policy Administrator may define and modify the behaviour of a Message Policy
b) A CSDS Message Policy Selector may select and activate a Message Policy and stop/re-start a Policy Engine
c) A CSDS Queue Manager may release or discard held messages and stop/re-start a Policy Engine.

6.1.6 Encryption

CRYPTO-1: There shall be an interface to cryptographic functions that perform the following operations in accordance with RFC 2630:

a) RSA asymmetric encryption and digital signature operations
b) DSA digital signature operations
c) Diffie-Hellman asymmetric encryption operations
d) Triple DES symmetric encryption operations.

6.1.7 Label Checking

LABEL-1: There shall be an interface to message security label checking functions that perform the following operations:

a) Check the validity of a given label
b) Check that the given label is dominated by a specified clearance.

6.1.8 Virus Scanning

VS-1: There shall be an interface that calls appropriate Virus Scanner filters correctly.

6.2 Assurance Measures

This section describes how the assurance requirements will be met.

- **Measures Used to Meet Component: ACM_AUT.1**

  This requirement will be met by documentation describing the Configuration Management system used during the development of the TOE.
- **Measures Used to Meet Component: ACM_CAP.4**

  This requirement will be met by documentation describing the Configuration Management system used during the development of the TOE.
- **Measures Used to Meet Component: ACM_SCP.2**

  This requirement will be met by documentation describing the Configuration Management system used during the development of the TOE.
- **Measures Used to Meet Component: ADO_DEL.2**

  This requirement will be met by documentation describing the Trusted delivery of the TOE.
- **Measures Used to Meet Component: ADO_IGS.1**

  This requirement will be met by documentation describing the Installation, Generation and Start-up of the TOE.
- **Measures Used to Meet Component: ADV_FSP.2**

  This requirement will be met by documentation describing the functional specification for the TOE supported by the Security Target and Administration documentation.
- **Measures Used to Meet Component: ADV_HLD.2**

  This requirement will be met by the high level design for the TOE supported by the Security Target.
- **Measures Used to Meet Component: ADV_IMP.1**

  This requirement will be met by the source code for the TOE supported by the Security Target.
- **Measures Used to Meet Component: ADV_LLD.1**

  This requirement will be met by the low-level design for the TOE supported by the Security Target.
- **Measures Used to Meet Component: ADV_RCR.1**

  This requirement will be met by information in the functional specification, high-level design, low-level design and source code for the TOE supported by the Security Target which will demonstrate correspondence between the levels of design and implementation representations.
- **Measures Used to Meet Component: ADV_SPM.1**

  This requirement will be met by the Security Target (this document).
- **Measures Used to Meet Component: AGD_ADM.1**

  This requirement will be met by the Administration documentation supported by the Security Target, documentation describing the functional specification, high-level design, installation, guidance and start-up documentation, and the life-cycle definition documents.

- **Measures Used to Meet Component: AGD_USR.1**

  This assurance component will not be applicable to this evaluation as there are no direct users of the TOE but is included for completeness of the EAL4 assurance requirements.
- **Measures Used to Meet Component: ALC_DVS.1**

  This assurance requirement will be met by the documentation describing the developer security measures.
- **Measures Used to Meet Component: ALC_LCD.1**

  This assurance requirement will be met by the lifecycle documentation.
- **Measures Used to Meet Component: ALC_TAT.1**

  This assurance requirement will be met by the development tools documentation and the source code.
- **Measures Used to Meet Component: ATE_COV.2**

  This assurance requirement will be met by the documentation describing the functional specification, test documentation and test coverage analysis.
- **Measures Used to Meet Component: ATE_DPT.1**

  This assurance requirement will be met by the documentation describing functional specification, high-level design, test documentation and depth of testing analysis.
- **Measures Used to Meet Component: ATE_FUN.1**

  This assurance requirement will be met by the documentation describing the functional specification, test documentation and procedures.
- **Measures Used to Meet Component: ATE_IND.2**

  This assurance requirement will be met by all the evaluation deliverables and a TOE suitable for testing.
- **Measures Used to Meet Component: AVA_MSU.2**

  This assurance requirement will be met by the Misuse Analysis supported by the other evaluation deliverables.
- **Measures Used to Meet Component: AVA_SOF.1**

  This assurance requirement will be met by Strength of Function Analysis and the other evaluation deliverables.
- **Measures Used to Meet Component: AVA_VLA.2**

  This assurance requirement will be met by Vulnerability Analysis, the other evaluation deliverables and a copy of the TOE suitable for testing.

7 Rationale

7.1 Security Objectives Rationale

7.1.1 Overview

Table 7-1 provides a mapping between the security objectives and the threats, assumptions and policies. It demonstrates that all the security objectives are required in order to cover the assumptions (see 7.1.2), counter the threats (see 7.1.3) and meet the policies (see 7.1.4).

Table 7-1 Mapping the TOE Security Environment to Security Objectives

Assumption/Threat/Policy	Objectives
A.Access_to_Passwords	OE.Access_to_Passwords, OE.SecFun
A.Admin_Docs	OE.Admin_Docs
A.Competent_Admin	OE.Admin
A.No_Abuse_By_Admin	OE.Admin
A.Prot_Against_Nature	OE.Prot_Against_Nature, OE.SecSta
A.Prot_Angst_Pwr_Fail	OE.Prot_Angst_Pwr_Fail, OE.SecSta
A.Platform_Admin	OE.Platform_Admin
A.Policy_Admin	OE.Policy_Admin
A.Remote_Admin	OE.Remote_Admin, OE.NoRemo
A.Remote_Admin_Env	OE.Remote_Admin_Env
A.Remote_Message_Policy	OE.Remote_Message_Policy
A.Review_Audit_Log	OE.Review_Audit_Log
A.DMZ.Protection	OE.DMZ_Protection,
A.DMZ_Separation	OE.DMZ_Separation
A.DOS_Protection	OE.DOS_Protection
A.Crypto_Keys	OE.Crypto_Keys
T.Admin_UserPriv	O.Accountability, O.Audit_Records, O.IDAuth, OE.IDAuth, OE.Admin, OE.Accountability, OE.Auditing
T.Hack_AC	O.Accountability, O.Audit_Records, O.IDAuth, OE.IDAuth, OE.NoRemo, OE.DMZ_Protection, OE.Accountability, OE.Auditing
T.Hack_Avl_Resource	OE.DOS_Protection

Assumption/Threat/Policy	Objectives
T.Hack_Masq	O.Accountability, O.Audit_Records, O.IDAuth, O.Mediat, OE.IDAuth, OE.NoRemo, OE.Remote_Admin, OE.Remote_Admin_Env, OE.DMZ_Protection, OE.Accountability, OE.Auditing
T.Inapprop_Rel_Info	O.Controlled_Flow, O.Mediat, OE.ConFlo, OE.Residual_info
P.Accountability	O.Accountability, O.Audit_Records, O.IDAuth, OE.IDAuth, OE.Accountability, OE.Auditing
P.Authorized_Use	O.IDAuth, O.SecFun, O.Mediat, OE.IDAuth. OE.Admin, OE.SecFun
P.Marking	O.Controlled_Flow, O.Mediat, OE.Label_Check
P.Physical_Control	OE.Physical_Control
P.Crypto	O.Crypto, OE.Crypto_Ops, OE.Crypto_Keys
P.Info_Flow_Control	O.Controlled_Flow, O.SecFun, O.Mediat, OE.ConFlo, OE.Residual_info
P.Anti_Virus	O.Anti_Virus, OE.Anti_Virus

7.1.2 Assumptions

The following demonstrates that the assumptions are covered by the security objectives for the environment.

A.Access_to_Passwords: Authorised administrator access to passwords
Cryptographic keys and root certificates must be protected so that authorised administrators can neither access nor modify them outside of authorised TOE IT Environment functions.

The coverage of A.Access_to_Passwords by OE.Access_to_Passwords is self evident. OE.SecFun also partly covers A.Access_to_Passwords by providing TOE IT Environment functions that enable authorised administrators to manage passwords.

A.Admin_Docs: Documentation for authorised administrators
Authorised administrators must follow the policies and procedures defined in the TOE documentation for secure administration of the TOE.

The coverage of A.Admin_Docs by OE.Admin_Docs is self evident.

A.Competent_Admin: Competent authorised administrators
Authorised administrators must be competent to manage the TOE and the security of the information it contains.

The coverage of A.Competent_Admin by OE.Admin is self evident.

A.No_Abuse_By_Admin: No abuse of authority by authorised administrators
Authorised administrators must be trusted not to abuse their authority.

OE.Admin covers A.No_Abuse_By_Admin since it requires that authorised administrators are competent and trustworthy.

A.Prot_Against_Nature: Natural disaster protection
The system must be adequately protected against natural disasters such as fires and floods (e.g., sprinkler systems, alarms, etc.).

The coverage of A.Prot_Against_Nature by OE.Prot_Against_Nature is self evident.
OE.SecSta also partly covers A.Prot_Against_Nature by ensuring that the IT environment does not compromise its resources on recovery from an interruption in TOE service.

A.Prot_Agnst_Pwr_Fail: Power failure protection
The system must have adequate backup power sources to ensure that sudden losses of power do not affect availability of service or loss of data.

The coverage of A.Prot_Agnst_Pwr_Fail by OE.Prot_Agnst_Pwr_Fail is self evident.
OE.SecSta also partly covers A.Prot_Agnst_Pwr_Fail by ensuring that the IT environment does not compromise its resources on recovery from an interruption in TOE service.

A.Platform_Admin: Platform administration
Administration of the CSB2 and TSOL platform must be performed locally and not via a DMZ network.

The coverage of A.Platform_Admin by OE.Platform_Admin is self evident.

A.Policy_Admin: Policy administration
Authorised administrators acting in the role of a CSDS Message Policy Administrator shall perform the role either exclusively locally via the DMZ network or exclusively remotely.

The coverage of A.Policy_Admin by OE.Policy_Admin is self evident.

A.Remote_Admin: Remote administration
CSDS Message Policy Administrators outside the DMZ network shall only be able to define and modify Message Policy settings, and only via networks connected to the DMZ network.

The coverage of A.Remote_Admin by OE.Remote_Admin is self evident.
OE.NoRemo also partly covers A.Remote_Admin by ensuring that authorised administrators cannot access the TOE or the IT environment directly from the internal or external subscriber networks.

A.Remote_Admin_Env: Remote administration environment
Authorised administrators outside the DMZ network shall operate in a controlled and well-managed environment which restricts definition and modification of Message Policy to authorised CSDS Message Policy Administrators and affords an equivalent level of protection as that required for the DMZ network environment.

The coverage of A.Remote_Admin_Env by OE.Remote_Admin_Env is self evident.

A.Remote_Message_Policy: Remote Message Policy Integrity
The integrity of Message Policies transferred from a remote DSA to a DSA on the DMZ network must be protected by digital signatures, which are verified by the crypto subsystem provided by the IT environment.

The coverage of A.Remote_Message_Policy by OE.Remote_Message_Policy is self evident.

A.Review_Audit_Log: Authorised administrators review audit logs
Authorised administrators shall review audit logs regularly.

The coverage of A.Review_Audit_Log by OE.Review_Audit_Log is self evident.

A.DMZ_Protection: Adequate protection of the DMZ
The DMZ network must be protected. The DMZ network must be protected from any other connected network by an appropriately assured (up to EAL4/E3) and configured boundary separation device.

The coverage of A.DMZ_Protection by OE.DMZ_Protection is self evident.

A.DMZ_Separation: Separation of the DMZ for each direction of flow
DMZ network(s) connected to one or more Policy Servers on different instances of CSDS that are controlling message flow in the same direction (i.e. from Company to World, or from World to Company) must not share the same DMZ network(s) as the Policy Servers controlling message flow in the other direction.

The coverage of A.DMZ_Separation by OE.DMZ_Separation is self evident.

A.DOS_Protection: Protection against Denial of Service
The CSDS must be protected against Denial of Service attacks. This might be by a border MTA protected by a packet firewall.

The coverage of A.DOS_Protection by OE.DOS_Protection is self evident.

A.Crypto_Keys: Crypto Key Management
Authorised administrators shall enter, maintain and delete cryptographic keys in a secure manner.

The coverage of A.Crypto_Keys by OE.Crypto_Keys is self evident.

7.1.3 Threats

The following demonstrates that the threats are countered by the security objectives for the TOE.

T.Admin_UserPriv: Administrator violates user privacy policy

An authorised administrator learns the identity (or other privacy related information) of user(s) in violation of subscriber privacy policy. Privacy-related information is sensitive information associated with the identity of a user.

T.Admin_UserPriv is countered by:

a) O.Accountability and OE.Accountability require that all activities are audited hence increasing the chance of detection
b) O.Audit_Records and OE.Auditing require that the audit trail can be read and searched for events
c) O.IDAuth and OE.IDAuth require that all administrators are uniquely identified and hence can be positively associated with audit records
d) OE.Admin requires that administrators are trustworthy, so reducing the likelihood of attempts to access privacy related information.

T.Hack_AC: Hacker undetected system access

A hacker gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability.

T.Hack_AC is countered by:

a) O.Accountability and OE.Accountability require that all activities are audited hence increasing the chance of detection
b) O.Audit_Records and OE.Auditing require that the audit trail can be read and searched for events
c) O.IDAuth and OE.IDAuth require that all administrators are uniquely identified and hence can be positively associated with audit records
d) OE.NoRemo reduces the risk of an attack being launched from the internal or external subscriber networks
e) OE.DMZ_Protection reduces the risk of an attack being launched from the DMZ.

T.Hack_Avl_Resource: Hacker attempts resource denial of service

A hacker executes commands, sends data, or performs other operations that make system resources unavailable to system users. Resources that may be denied to users include bandwidth, processor time, memory, and data storage.

T.Hack_Avl_Resource is countered by:

a) OE.DOS_Protection assumes that protection against Denial of Services attacks is provided by the environment in which the TOE operates.

T.Hack_Masq: Hacker masquerading as a legitimate user or as system process

A hacker masquerades as a subscriber or administrator to perform operations that will be attributed to the subscriber or administrator or a system process.

T.Hack_Masq is countered by:

a) O.Accountability and OE.Accountability require that all activities are audited hence increasing the chance of detection
b) O.Audit_Records and OE.Auditing require that the audit trail can be read and searched for events
c) O.IDAuth and OE.IDAuth require that all administrators are uniquely identified and hence can be positively associated with audit records
d) O.Mediat requires that only permitted types of information flow between networks
e) OE.NoRemo reduces the risk of an attack being launched from the internal or external subscriber networks
f) OE.Remote_Admin and OE.Remote_Admin_Env reduce the risk of an attack being launched by an attacker masquerading as an authorised remote administrator
g) OE.DMZ_Protection reduces the risk of an attack being launched from the DMZ.

T.Inapprop_Rel_Info: Inappropriate release of information

Unauthorised release of information from the DMZ into a subscriber network.

T.Inapprop_Rel_Info is countered by:

a) O.Controlled_Flow requires that all information passing between the networks passes through the Policy Engine
b) O.Mediat requires that only permitted information types can be passed to a network
c) OE.ConFlo ensures that information flowing between the two subscriber networks cannot bypass the Policy Engine
d) OE.Residual_info ensures that information from a previous information flow is not available.

7.1.4 Policies

The following demonstrates that the organisational security policies are met by the security objectives for the TOE.

P.Accountability: Individual accountability

Individuals shall be held accountable for their actions.

P.Accountability is met by:

a) O.IDAuth and OE.IDAuth which specifies that each administrator is uniquely identified before being granted direct access to the TOE
b) O.Accountability and OE.Accountability require that each message can be associated with a subscriber and administrator use of security related functions is recorded
c) O.Audit_Records and OE.Auditing require that the audit trail can be read and searched for events.

P.Authorized_Use: Authorised use of information

Information shall be used only for its authorised purpose(s).

P.Authorized_Use is met by:

a) O.IDAuth and OE.IDAuth which specifies that each administrator is uniquely identified before being granted direct access to the TOE
b) O.SecFun and OE.SecFun require that authorised administrators are able to manage the TOE
c) O.Mediat requires that only permitted information types can be passed to a network
d) OE.Admin requires that administrators are trustworthy.

P.Marking: Information marking

Information shall be appropriately marked with an appropriate label.

P.Marking is met by:

a) O.Controlled_Flow requires that information is properly controlled as it passes between networks
b) O.Mediat requires that only permitted types of information flow between networks hence ensuring that labelling is maintained
c) OE.Label_Check requires that labels are valid and dominated by a specified clearance.

P.Physical_Control: Physical protection

Information shall be physically protected to prevent unauthorised disclosure, destruction, or modification.

P.Physical_Control is met by:

a) OE.Physical_Control requires that the TOE is physically protected.

P.Crypto: Cryptographic Protection

Cryptographic operations shall be performed in a secure manner. This shall include entering and deleting of cryptographic keys.

P.Crypto is met by:

a) O.Crypto provides for correct handling of cryptographic operations
b) OE.Crypto_Ops provides correct cryptographic operations for the TOE to use
c) OE.Crypto_Keys ensures that cryptographic keys are handled in a secure manner.

P.Info_Flow_Control: Control of Information Flow
Information shall be protected to prevent unauthorised flow of information.

P.Info_Flow_Control is met by:

a) O.Controlled_Flow ensures that information must flow through the Policy Engine
b) O.SecFun ensures that Message Policy can only be changed in an authorised manner
c) O.Mediat requires that only permitted information types can be passed to a network
d) OE.ConFlo ensures that information flowing between the two subscriber networks cannot bypass the Policy Engine
e) OE.Residual_info ensures that information from a previous information flow is not available.

P.Anti_Virus: Virus Scanner Filters
It shall be possible to scan subscriber message elements for malicious code corresponding to a set of malicious code definitions.

P.Anti_Virus is self evidently met by O.Anti_Virus and OE.Anti_Virus.

7.2 Security Requirements Rationale

7.2.1 Rationale for completeness of TOE Security Functions

7.2.1.1 TOE Security Functional Requirements meet the TOE Security Objectives

Table 7-2 provides a mapping between security objectives for the TOE and TOE security functional requirements (SFRs).

Table 7-2 – TOE Security Functional Requirement to Security Objective Mapping

Objectives	Requirements
O.Accountability	FAU_GEN.1, FAU_GEN.2
O.Audit_Records	FAU_GEN.1, FAU_GEN.2
O.Controlled_Flow	FDP_IFC.1, FDP_IFF.1,
O.IDAuth	FIA_UAU.2X, FIA_UID.2X
O.SecFun	FMT_MSA.1, FMT_SMF.1, FMT_SMR.1
O.Mediat	FCS_COP.1X, FDP_IFC.1, FDP_IFF.1, FDP_LCK.1X, FMC_VSF.1X, FMT_MSA.3X
O.Crypto	FCS_COP.1X
O.Anti_Virus	FMC_VSF.1X

The following demonstrates that all of the SFRs are required and suitable to meet the security objectives:

O.Accountability: Accountability of Information Flows
The TOE must provide user accountability of information flows through the TOE and for authorised administrator use of security related functions.

FAU_GEN.1and FAU_GEN.2 ensure that all Message transactions and all actions performed by authorised administrators can be configured to generate audit records.

O.Audit_Records: Record Readable Audit Trail
The TOE must provide a means to record a readable audit trail of security related events, with accurate dates and times.

FAU_GEN.1and FAU_GEN.2 ensure that all Message transactions and all actions performed by authorised administrators can be configured to generate audit records with accurate dates and times.

O.Controlled_Flow: Controlled Information Flow
Information cannot flow through the TOE between two subscriber networks unless it passes through the Policy Engine.

SFRs FDP_IFC.1 and FDP_IFF.1 defines an information flow control policy, attributes and rules which meet security objective O.Controlled_Flow by ensuring that all messages received from a network traverse the TOE through pre-defined channels which guarantee attention by the Policy Engine in the configured DMZ subsystems.

O.IDAuth: Unique Identity and Authentication
The TOE must uniquely identify and authenticate the claimed identity of all TOE authorised administrators before granting them access to TOE functions. The TOE must protect the authenticity of any Message Policy change made by an authorised administrator.

FIA_UAU.2X and FIA_UID.2X ensure that all users of the TOE are identified and authenticated as authorised administrators before any other actions are allowed. Changes to Message Policy may only be downloaded by identified and authenticated authorised administrators.

O.SecFun: Secure Administration Functions
The TOE must provide functionality that enables authorised administrators to manage the TOE security functions.

FMT_SMR.1 ensures that the TOE maintains three distinct authorised administrator roles for Policy Engine queue management, Message Policy selection and Message Policy administration. FMT_MSA.1 and FMT_SMF.1provide role specific security functions to manage Policy Engine queues and to select and administer a Message Policy.

O.Mediat: Mediation of Flow of Information
The TOE must mediate the flow of all information between connected subscriber networks governed by the TOE, in accordance with the Message Policy, ensuring that checks and actions are invoked in accordance with specific security attributes of each subscriber message.

However, the enforcement of the checks and actions is excluded from the scope of the evaluation.

FDP_IFC.1 and FDP_IFF.1 ensure that all subscriber messages flowing between the subscriber networks connected to the TOE are mediated by the Policy Engine in accordance with the active Message Policy, which rejects (non-delivers) or holds messages that do not conform to the Message Policy and adjusts labels and security attributes as required. FCS_COP.1X ensures that cryptographic operations associated with the S/MIME content of messages are handled correctly. FDP_LCK.1X ensures that label checking operations are called correctly. FMC_VSF.1X ensures that Virus Scanner filters are called correctly when required to scan for viruses in subscriber message elements. FMT_MSA.3X ensures that no subscriber message flow is permitted prior to the selection and activation of a Message Policy.

O.Crypto: Cryptographic Operations
The TOE must ensure that cryptographic operations are correctly handled.

FCS_COP.1X ensures that cryptographic operations invoked by the TOE are called correctly.

O.Anti_Virus: Virus Scanner Filters
The TOE must enable scanning of subscriber message elements for malicious code as required by the Message Policy.

FMC_VSF.1X ensures that Virus Scanner filters are called correctly when required to scan for viruses in subscriber message elements.

7.2.1.2 IT Environment SFRs meet the IT Environment Security Objectives

As stated in Section 5.3.1, the TOE relies on SFRs specified in Sections 5.3.2, 5.3.3, and 5.3.4 which define the requirements for cryptographic operations and associated key management, label checking operations and virus scanning to be supplied, respectively, by a crypto subsystem, a label subsystem and VS filters. Table 7-3 provides a mapping between the relevant CSDS security objectives for the IT environment and the SFRs for the IT environment specified in Sections 5.3.2, 5.3.3 and 5.3.4. The justification that the identified SFRs are required and suitable to meet the IT Environment objectives is self-evident.

As specified in Section 5.3.1, the TOE relies on the use of the crypto subsystem digital signature operations to verify the integrity of Message Policies received from a remote DSA (via a DSA on the DMZ network). This is expressed as the IT environment security objective OE.Remote_Message_Policy, which is met by the IT environment SFR FPT_ITI.1 and its dependency on FCS_COP.1, the security requirements for which are described in Section 5.3.5.

Table 7-3 – CSDS Security Objectives for the IT Environment to Section 5.3.2, 5.3.3 5.3.4 and 5.3.5 SFR Mapping

CSDS Security Objectives for the IT Environment	SFRs for the IT Environment Specified in Section 5.3.2, 5.3.3, 5.3.4 and 5.3.5
OE.Crypto_Ops	FCS_COP.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.4.
OE.Label_Check	FDP_LCK.2X

CSDS Security Objectives for the IT Environment	SFRs for the IT Environment Specified in Section 5.3.2, 5.3.3, 5.3.4 and 5.3.5
OE.Anti_Virus	FMC_VSF.2X
OE.Remote_Message_Policy	FPT_ITI.1

As stated in Section 5.3.1, the TOE relies on selected CSB2 SFRs. Table 7-4 provides a mapping between the CSDS security objectives for the IT environment and the CSB2 SFRs. The justification that the identified CSB2 SFRs are required and suitable to meet the CSB2 TOE objectives is self-evident.

Table 7-4 – CSDS Security Objectives for the IT Environment to CSB2 SFR Mapping

CSDS Security Objectives for the IT Environment	CSB2 SFRs
OE.ConFlo	FDP_IFC.1, FDP_IFF.1, FMT_MOF.1
OE.SecFun	FMT_MOF.1, FMT_SMR.4
OE.Accountability	FAU_GEN.4

As stated in Section 5.3.1, the TOE relies on all of the TSOL SFRs that are required to comply with [LSPP] and [RBAC] protection profiles. Table 7-5 provides a mapping between the CSDS security objectives for the IT environment and the relevant [LSPP] and [RBAC] security objectives, thus providing an implicit mapping to the TSOL TOE security functional requirements (SFRs).

Please refer to [LSPP] and [RBAC] for a full specification of [LSPP] and [RBAC] SFRs, and justification that they are required and suitable to meet [LSPP] and [RBAC] objectives.

Table 7-5 – CSDS Security Objectives for the IT Environment to [LSPP] and [RBAC] Security Objective Mapping

CSDS Security Objectives for the IT Environment	TSOL TOE security objectives
OE.ConFlo	O.MANDATORY_ACCESS, O.ENFORCEMENT
OE.IDAuth	O.AUTHORISATION
OE.NoRemo	O. MANDATORY_ACCESS, O.ENFORCEMENT
OE.SecFun	O.MANAGE, O.DUTY, O.HIERARCHICAL, O.ROLE, O.DISCRETIONARY_ACCESS, O.ENFORCEMENT
OE.Access_to_Passwords	O.MANDATORY_ACCESS, O.DISCRETIONARY_ACCESS, O.ENFORCEMENT
OE.SecSta	O.MANAGE, O.ENFORCEMENT
OE.Residual_info	O.RESIDUAL_INFORMATION

CSDS Security Objectives for the IT Environment	TSOL TOE security objectives
OE.Accountability	O.AUDITING
OE.Auditing	O.AUDITING

As specified in Section 5.3.1, the TOE relies on the IT environment to protect the TOE and the CSB2/TSOL platform from specific attacks originating from the subscriber networks and networks attached to a DMZ network. Section 5.3.1 lists the minimum set of SFRs taken from [CC] Part 2 that are required to provide the necessary protection, as well as the associated security objectives for the IT environment. The minimum set of SFRs is based on the assumption that a packet firewall is required for each of the subscriber networks and an appropriate boundary separation device (packet firewall; application firewall) is required for each of the DMZ networks, implementing information flow control policies with administrator access control and auditing.

7.2.2 Internal Consistency of Requirements

The SFR FCS_COP.1X component is explicitly stated. It is an additional function that is necessary because it effectively provides a generic API to the [CC] Part 2 component FCS_COP.1, which is provided by the IT environment. It is hierarchical to no other component and has one dependency, FCS_COP.1, met by the IT environment. The EAL4 assurance requirements are fully applicable to FCS_COP.1X.

The SFR FDP_LCK.1X component is explicitly stated. It is an additional function that is necessary because it specifies the requirement to call label checking operations, which are provided by the IT environment. It is hierarchical to no other component and has one dependency, FDP_LCK.2X, met by the IT environment. The EAL4 assurance requirements are fully applicable to FDP_LCK.1X.

The SFR FMC_VSF.1X component is an explicitly stated component of an extended class handling malicious code. It is an additional function that is necessary because it specifies the requirement to call virus scanning operations, which are provided by the IT environment. It is hierarchical to no other component and has one dependency, FMC_VSF.2X, met by the IT environment. The EAL4 assurance requirements are fully applicable to FMC_VSF.1X.

The SFR FMT_MSA.3X component is explicitly stated. It is a modified version of the [CC] Part 2 component FMT_MSA.3. The modification is required, as the ability to override default values when an object or information is created (as required by FMT_MSA.3.2) is not applicable to the TOE. FMT_MSA.3X is necessary because it specifies the requirement that no subscriber message flow shall be permitted prior to selection and activation of a Message Policy. It is hierarchical to no other component and has one dependency, FMT_MSA.1. The EAL4 assurance requirements are fully applicable to FMT_MSA.3X.

The SFR components FIA_UID.2X and FIA_UAU.2X are explicitly stated. They are additional functions that are necessary because although they require identification & authentication of users, the actual identification and authentication functions are performed by FCS_COP.1X. They are hierarchical to no other component and the only dependency is of each on FCS_COP.1X. The EAL4 assurance requirements are fully applicable to FIA_UID.2X and FIA_UAU.2X.

SFR FAU_GEN.2 is refined by adding an additional dependency (see Section 7.2.3). The refinement does not alter the list of dependencies of the original requirement.

Apart from the explicitly stated components, TOE SFRs comply with [CC] Part 2, with all required operations of assignment, selection and refinement performed to make the requirements TOE specific. The assignment, selection and refinement operations were performed using consistent computer security and TOE specific terminology. Hence the SFRs are internally consistent. Where relevant, the TOE SFRs are mutually supportive, in accordance with their dependencies.

7.2.3 Dependency Rationale

Table 7-6 demonstrates that all the TOE requirement dependencies are met or provides an explanation of why the dependency is inappropriate.

Table 7-6 TOE Requirement Dependencies

Requirement	Dependencies
FAU_GEN.1	FPT_STM.1. This dependency is met by the TSOL TOE.
FAU_GEN.2	FAU_GEN.1, FIA_UID.1, FDP_IFF.1. The dependency on FIA_UID.1 is met by FIA_UID.2X. Dependency on FDP_IFF.1 is added for the case of message transaction, where the user causing the event, identified by the Policy Engine, is the subscriber that sends the message.
FCS_COP.1X	FCS_COP.1. This dependency is met by the IT environment.
FDP_IFC.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3. The dependency on FMT_MSA.3 is met by FMT_MSA.3X.
FDP_LCK.1X	FDP_LCK.2X. This dependency is met by the IT environment.
FIA_UAU.2X	FCS_COP.1X
FIA_UID.2X	FCS_COP.1X
FMC_VSF.1X	FMC_VSF.2X. This dependency is met by the IT environment.
FMT_MSA.1	FDP_IFC.1, FMT_SMF.1, FMT_SMR.1
FMT_MSA.3X	FMT_MSA.1
FMT_SMF.1	-
FMT_SMR.1	FIA_UID.1. The dependency on FIA_UID.1 is met by FIA_UID.2X.

As can be seen from Table 7-6 all dependencies are met, or where dependencies are not met the dependency is inappropriate for the environment in which the TOE is to be used.

Table 7-7 demonstrates that all the IT environment requirement dependencies are met or provides an explanation of why the dependency is inappropriate.

Table 7-7 IT Environment Requirement Dependencies

Requirement	Dependencies
For Packet Firewall and Boundary Separation Device:	
FAU_GEN.1	FPT_STM.1
FAU_SAR.1	FAU_GEN.1
FDP_IFC.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3
FIA_UAU.1	FIA_UID.1
FIA_UID.1	-
FMT_MSA.1	FDP_IFC.1, FMT_SMF.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1
FMT_SMF.1	-
FMT_SMR.1	FIA_UID.1
FPT_STM.1	-
For Cryptographic Support	
FCS_CKM.1	FCS_CKM.4, FCS_COP.1, FMT_MSA.2 (Met instead by OE.Crypto_Keys)
FCS_CKM.2	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2 (Met instead by OE.Crypto_Keys)
FCS_CKM.4	FCS_CKM.1, FMT_MSA.2 (Met instead by OE.Crypto_Keys)
FCS_COP.1	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2 (Met instead by OE.Crypto_Keys)
For Label Checking Operations	
FDP_LCK.2X	-
For Virus Scanner Filters	
FMC_VSF.2X	-
For Inter-TSF Detection of Modification	
FPT_ITI.1	FCS_COP.1

As can be seen from Table 7-7 all dependencies are met, or where dependencies are not met the dependency is inappropriate for the environment in which the IT environment is to be used.

7.2.4 Justification of Assurance Level

This security target was developed for a generalised environment with moderate risk to the assets and as such an assurance level of EAL4 was deemed to be appropriate.

7.2.5 Justification of the Strength of Function Claim

There are no mechanisms that require evaluation in the TOE therefore it is appropriate that no claim is made.

7.3 TOE Summary Specification Rationale

7.3.1 Satisfaction of TOE Security Functional Requirements

Table 7-8 demonstrates that the combination of specified TOE security functions work together to satisfy the TOE security functional requirements.

Table 7-8 Mapping of TOE Security Functional Requirement to TOE Security Function

TOE Security Functional Requirement	TOE Security Functions
FAU_GEN.1	AUD-1, AUD-2
FAU_GEN.2	AUD-1, AUD-2
FCS_COP.1X	CRYPTO-1, CERT-1
FDP_IFC.1	POL-1, POL-2
FDP_IFF.1	POL-1, POL-2
FDP_LCK.1X	LABEL-1
FIA_UAU.2X	I&A-1
FIA_UID.2X	I&A-1
FMC_VSF.1X	VS-1
FMT_MSA.1	AC-1
FMT_MSA.3X	POL-2
FMT_SMF.1	AC-1
FMT_SMR.1	AC-1

FAU_GEN.1 requires that the TSF can generate audit records when defined events occur. AUD-1 ensures that suitable records are taken and AUD-2 specifies the information that is contained in each record.

FAU_GEN.2 requires that each auditable event is attributable to a user. AUD-1 and AUD-2 ensure that records of auditable events contain the identity of the user that initiated the event.

FCS_COP.1X requires that calls to cryptographic operations performed by the IT environment are properly formed. CRYPTO-1 provides a well defined generic interface (API) to RFC 2630 compliant cryptographic operations provided as a vendor specific library. CERT-1 provides an interface to cryptographic functions that validate the certificate paths associated with subscriber messages.

FDP_IFC.1 requires that all messages are subject to the CSDS Message Flow Control Policy. POL-1 and POL-2 ensure that the Message Policy is applied to all subscriber messages.

FDP_IFF.1 requires that the CSDS Message Flow Control Policy is applied to all subscriber messages flowing through the TOE. POL-1 and POL-2 ensure that this is the case.

FDP_LCK.1X requires that calls to label checking operations performed by the IT environment are properly formed. LABEL-1 calls operations which check that a given label is valid and dominated by a specified clearance.

FIA_UAU.2X requires that all users of the TOE are authenticated. I&A-1 identifies and authenticates users using individual authenticated certificates.

FIA_UID.2X requires that all user of the TOE are identified. I&A-1 identifies and authenticates users using individual authenticated certificates.

FMC_VSF.1X requires that calls to virus scanning operations performed by the IT environment are properly formed. VS-1 calls appropriate Virus Scanner filters correctly.

FMT_MSA.1 requires restriction on specific functions for specific roles to manage Message Policy and to release or discard subscriber messages from manual queues. AC-1 provides these functions and restricts them to the defined roles.

FMT_MSA.3X requires that no subscriber message flow is permitted prior to the selection and activation of a Message Policy. POL-2 provides this function.

FMT_SMF.1 requires specific functions to manage Message Policy and Policy Engine queues. AC-1 provides these functions and restricts them to the defined roles.

FMT_SMR.1 requires that there are defined roles associated with users. AC-1 ensures that all users interact with the TOE using defined roles.

7.3.2 Justification of Compliance with Assurance Requirements

The compliance of assurance measures with assurance requirements is demonstrated in Section 6.2.

Annex A
Rationale for alternative crypto subsystem

CSDS accesses the installed crypto subsystem through a well-defined interface, which is fully specified in terms of effects, exceptions and error messages.

The CSDS TOE was evaluated using each of the 'Cryptomathic PrimeInk Premium VIC for CSDS' Pkg Vn 1.0.07, the 'SFL VIC for CSDS' Pkg Vn 3.0.36 and the 'Null VIC for CSDS' Pkg Vn 3.0.36 crypto subsystems. However the scope of the TOE is such that the focus of the evaluation, with respect to each subsystem, was on the TOE invoking use of the subsystem and acting on responses received from it. The interface to the subsystems was evaluated in the course of this activity.

The evaluated CSDS TOE can be used in conjunction with one of a number of crypto subsystem options. Whilst the crypto subsystem itself is not within the scope of this TOE, Clearswift undertakes a number of activities to ensure provision of quality customer solutions which include:

- Use of crypto subsystems that it considers reputable.
- Testing to exercise the use of each crypto subsystem in conjunction with CSDS. This testing includes authentication of CSDS users by the CSDS Administration and full testing of the CSDS Message Flow Control Policy using various configurations of the Message Policy, and fully exercising the subsystem interface. It is conducted under Clearswift's accredited quality system, with test records made and provision existing to address any unexpected results.
- Willingness to discuss relevant test findings with specific customers.

Whilst performing the formal evaluation of the CSDS TOE, the evaluators were also given visibility of the above Clearswift testing process.

Annex B
Rationale for alternative label subsystem

CSDS accesses the installed label subsystem through a well-defined interface, which is fully specified in terms of effects, exceptions and error messages.

The CSDS TOE was evaluated using each of the 'X.841 LSL for CSDS' Pkg Vn 3.0.36 and the 'Null LSL for CSDS' Pkg Vn 3.0.36 label subsystems. However the scope of the TOE is such that the focus of the evaluation, with respect to each subsystem, was on the TOE invoking use of the subsystem and acting on responses received from it. The interface to the subsystems was evaluated in the course of this activity.

The evaluated CSDS TOE can be used in conjunction with one of a number of label subsystem options. Whilst the label subsystem itself is not within the scope of this TOE, Clearswift undertakes a number of activities to ensure provision of quality customer solutions which include:

- Use of label subsystems that it considers reputable.
- Testing to exercise the use of each label subsystem in conjunction with CSDS. This includes full testing of the CSDS Message Flow Control Policy using various configurations of the Message Policy, and fully exercising the subsystem interface. It is conducted under Clearswift's accredited quality system, with test records made and provision existing to address any unexpected results.
- Willingness to discuss relevant test findings with specific customers.

Whilst performing the formal evaluation of the CSDS TOE, the evaluators were also given visibility of the above Clearswift testing process.

Annex C
Rationale for alternative VS filters

The CSDS TOE was evaluated using each of the Sophos SAVI VS and CSAV command AV for Solaris VS filters. Each VS filter was developed by an independent company having no knowledge of the design of the Policy Engine. Each VS filter is COTS software with a history of successful use and few reported problems.

The evaluated CSDS TOE can be used in conjunction with between zero and four optional VS filters. Whilst the VS filter itself is not within the scope of this TOE, Clearswift undertakes a number of activities to ensure provision of quality customer solutions which include:

- Use of VS filters that it considers reputable.
- Testing to exercise the use of each VS filter in conjunction with CSDS. This includes full testing of the CSDS Message Flow Control Policy using various configurations of the Message Policy, and fully exercising the subsystem interface. It is conducted under Clearswift's accredited quality system, with test records made and provision existing to address any unexpected results.
- Willingness to discuss relevant test findings with specific customers.

Whilst performing the formal evaluation of the CSDS TOE, the evaluators were also given visibility of the above Clearswift testing process.