CLEARSWIFT™

# DeepSecure (CSDS) Release 2.1

# Security Target

| | |
|---|---|
| Document No: | DN11488/1 |
| Release Authority: | Clearswift |

# Copyright Notice

This document contains information that is the subject of copyright owned by or licensed to Clearswift. The contents of this document shall not be used, copied or disclosed, without the prior written consent of Clearswift.

# Table of Contents

# 1 Introduction

## 1.1 ST Identification

| | |
|---|---|
| Title: | Clearswift DeepSecure (CSDS) Security Target (ST) |
| Authors: | Ralph Worswick, Jim Craigie |
| CC Version: | 2.3 |
| ST Version | DN11488/1 |
| General Status: | Draft |
| TOE | Clearswift DeepSecure (CSDS) Release 2.1 |
| 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 DeepSecure. 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 policy 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 |
| Annex A | Describes the contents of a Message Policy |
| Annex B | Describes Policy Server configuration data |
| Annexes C to I | Provide rationale for the use of alternative versions of external libraries used by ClearPoint and the Policy Engine to manage and enforce aspects of Message Policy |
| Annexes J to L | Provide rationale for the use of alternative platforms to host the Policy Server, ClearPoint and the SPIF Editor. |

## 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 |
| CrT | Cryptographic Toolkit |
| CSB2 | Clearswift Bastion 2 |
| CSDS | Clearswift DeepSecure |
| DAP | Directory Access Protocol |
| DMZ | De-Militarised Zone |
| DN | Distinguished Name |
| DSA | Directory System Agent |
| DSN | Delivery Status Notification [RFC 3464] |
| EAL | Evaluation Assurance Level |
| GUI | Graphical User Interface |
| HTTP | Hypertext Transfer Protocol |
| IT | Information Technology |
| JVM | Java Virtual Machine |
| LDAP | Lightweight Directory Access Protocol |
| LSL | (Security) Label Support Library (an instantiation of the formal security label subsystem) |
| LSLI | Label Support Library API |
| MDN | Message Disposition Notification [RFC 3798] |
| MTA | Message Transfer Agent |
| OS | Operating System |
| PAA | Positive Action Assurance |
| PKI | Public Key Infrastructure |
| PP | Protection Profile |
| S/MIME | Secure/Multipurpose Internet Mail Extensions |
| SF | Security Function |
| SFP | Security Function Policy |

| Abbreviation | Meaning |
|---|---|
| SFR | Security Functional Requirement |
| SFL | S/MIME Freeware Library |
| SMTP | In this document the term SMTP follows colloquial usage to encompass both the *Simple Mail Transfer Protocol* defined in [RFC 2821] and the *Internet Message Format* defined in [RFC 2822] |
| SOAP | Simple Object Access Protocol |
| SOF | Strength of Function |
| SPIF | Security (Label) Policy Information File |
| SSL | Secure Sockets Layer |
| 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 (Library) |
| VICI | Vendor Independent Cryptographic API |
| VICL | VIC Library (an instantiation of the Cryptographic Subsystem) |
| VM | Virtual Machine |
| VS | Virus Scanner |
| XML | Extensible Markup Language |

## 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 Message Policy rules and attributes that mediate the flow of subscriber messages in accordance with the CSDS Message Flow Control Policy.

*Administration Service* The Policy Server component that provides the administrative functions required by the authorised CSDS Server-mode Administrators when using ClearPoint in Server-mode.

*Administrator Privilege* An aspect of administration of a Policy Server that may be permitted or denied to a specific CSDS Server-mode Administrator when using ClearPoint in Server-mode. A CSDS Server-mode Administrator may be granted more than one administrator privilege. Administrator privileges are: Message Policy Administration, Message Policy Selection, Message Policy Viewing, Policy Server Configuration Administration, Policy Server Configuration Viewing, Queue Management, Queue Viewing, Archive Viewing, Audit Log Viewing, and Diagnostic Log Configuration.

*ARCHIVE compartment** A type of DMZ compartment that contains the CSB2 trusted archive function.

*Authorised administrator* Sometimes just referred to as administrator. A human user who is known to, identified and authenticated by calls to the TOE or its IT environment prior to authorised access in one or more assigned roles for the purpose of managing the functions of the TOE or its IT environment. The following hierarchy of administrators and administrator roles are specifically named in this document:

- TOE administrator
    - CSDS Server-mode Administrator
    - CSDS Directory-mode Administrator
    - X.841 Security (Label) Policy Administrator
    - PKI Configuration Administrator[1]
- (IT Environment Administrator)
    - CSB2 Administrator
        - Acting in cots role associated with Policy Server
    - ClearPoint Management Station Administrator
    - SPIF Editor Platform Administrator.

*Certification Authority* An authority trusted by one or more users to create and assign public-key certificates. Optionally the certification authority may create the users' keys. [X.509]

*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.

*ClearPoint* The CSDS component which provides CSDS Server-mode Administrators and CSDS Directory-mode Administrators with an intuitive GUI interface, for administration of Message Policies and, CSDS Server-mode Administrators only, for Message Policy selection and activation, administration of subscriber message queues, archives, audit logs, diagnostic logs and stop/start of a Policy Engine. ClearPoint is a component of a ClearPoint Management Station.

*ClearPoint Management Station* A component of CSDS, comprising ClearPoint and external libraries, residing on a suitable hardware platform incorporating a Microsoft Windows OS.

[1] A PKI Configuration Administrator uses TOE components to manage PKI data (see SFR FMT_SMF). However, a PKI Configuration Administrator is identified and authenticated by the IT Environment, as a user of the IT environment authorised in that role and trusted to manage PKI data.

_ClearPoint Management Station Administrator_

An IT Environment Administrator permitted to manage, _inter alia_, ClearPoint PKI data, who is identified and authenticated by the ClearPoint Management Station, which could be achieved by a variety of means, including use of the Microsoft Windows OS; tokens on attached devices (e.g. smart cards); dedication of the ClearPoint Management Station to a single user.

_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 or assurance maintained version of Clearswift Bastion 2, also marketed as CS Bastion II, Clearswift Bastion 2.1 or Clearswift Bastion 2.2, compliant with the SFRs defined in [CSB2_ST].

_CSB2 Administrator_ An administrator identified and authenticated by TSOL and permitted, in accordance with specific CSB2 roles, to manage CSB2 compartments from a directly attached workstation.

_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_ Clearswift DeepSecure is an email policy management software suite that provides 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 Message Policy, the flow being determined from attributes of the subscriber message, including its originator and recipients. A CSDS deployment comprises one or more CSDS Servers, two or more ClearPoint Management Stations, and optionally one or more SPIF Editors, usually together with other components (not part of CSDS) including one or more X.509 Certification Authorities and an infrastructure of interconnected DSAs. CSDS encompasses the CSDS TOE together with components of CSDS that form part of the IT environment in this ST, although some of these IT environment components may be the subjects of independent evaluations, e.g. CSB2, TSOL.

*CSDS Directory-mode Administrator*

A TOE administrator authorised by a Policy Server to define and modify the behaviour of a Message Policy (using ClearPoint in Directory-mode).

*CSDS Message Flow Control Policy*

Defined by the content of the total set of TOE SFRs in Section 5.1 that reference it. It encompasses, but is wider in scope than the Message Policy.

*CSDS Server*

A component of CSDS, comprising two instantiations of Policy Server software, one Policy Server for each direction of message flow between the two subscriber networks. A CSDS Server is resident on a single CSB2/TSOL platform which forms part of the IT environment.

*CSDS Server-mode Administrator*

A TOE administrator, acting with specific administrator privileges, authorised by a Policy Server to define, modify, select and activate Message Policies, perform message release, non-delivery or discard actions, configure and view archives, audit logs and diagnostic logs and stop/start a Policy Engine (using ClearPoint in Server-mode).

*CSDS TOE*

The Clearswift DeepSecure Target of Evaluation comprises those functions and components of CSDS specified in Sections 2.5 and 2.6 of this Security Target. Other functions and components provided by CSDS form part of the IT environment in this ST.

*Data Type*

The type of data contained within a file, embedded object or message element.

*Directory-mode*

A mode of operation of ClearPoint in which CSDS Directory-mode Administrators define and modify Message Policy using a ClearPoint Management Station, and distribute to Policy Servers via one or more DSAs.

*Directory Synchronisation Agent*

The Policy Server component that downloads Message Policies stored in DSAs, validates their integrity and authenticates them against the user certificates held on the Policy Server for authorised CSDS Directory-mode Administrators. The Directory Synchronisation Agent may also download malicious code definition and spam definition updates from DSAs.

*Directory Synchronisation Uploader*

An IT environment component on a network connected to the DMZ network that uploades malicious code definition and spam definition updates to DSAs.

*Directory System Agent (DSA)*
Although specifically referring to an [X.500] Directory System Agent (DSA), the term DSA is used in this document to encompass both X.500 and other directory servers using DAP or LDAP protocols, such as an LDAP Server. A DSA may be used to store and distribute Message Policies, SPIFs, Certificates, Certificate Revocation Lists, malicious code definition and spam definition updates. The abbreviation DSA is also used in a few places to mean Digital Signature Algorithm, but this is clear from the context.

*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.

*Domain*
A collection of subscribers in the Company or World organisation to which a common set of Message Policy rules are to be applied (See Annex A, ‘Policy Tree’ for more information).

*External library*
A major library that is built and distributed independently of the TOE and forms part of the IT environment (except for the optional X.841 LSL external library, which is part of the TOE). Some external libraries include third party software.

*External interface*
An interface from the TOE to the IT environment. This includes interfaces to external libraries (except for the optional X.841 LSL external library, which is part of the TOE).

*Group*
A collection of subscribers in the Company or World organisation to which a common set of Message Policy rules are to be applied (See Annex A, ‘Policy Tree’ for more information).

*Message*
In this document, means a subscriber message or other messages originated by the Policy Engine.

*Message discard*
The Message Policy initiated event of permanent deletion of a subscriber message from a queue of type IN or the CSDS Server-mode Administrator initiated action of authorising permanent deletion of a subscriber message from a queue of type MANUAL, without sending notification messages or non-delivery reports to the message’s originator.

*Message element*
An atomic component of a message (or embedded message) derived from the decomposition of all structured formats that CSDS can decompose.

*Message non-deliver (reject)* The Message Policy initiated event of permanent deletion of a subscriber message from a queue of type IN or the CSDS Server-mode Administrator initiated action of authorising permanent deletion of a subscriber message from a queue of type MANUAL, sending applicable notification messages and non-delivery reports.

*Message Policy* A distinct configuration of the sets of rules and attributes that, when loaded into an instantiation of the Policy Engine (i.e. made the active Message Policy), defines the Message Policy rules and attributes that mediate the flow of subscriber messages in accordance with 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. The contents of a Message Policy are described in Annex A.

*Message release* The CSDS Server-mode Administrator initiated action of authorising movement of a subscriber message from a queue of type MANUAL to a queue of type COMPANY or WORLD.

*Message transaction* The set of events that occur during an application of the Message Policy rules and attributes that mediate the flow of subscriber messages in accordance with the CSDS Message Flow Control Policy.

*Originator/recipient (group) pair (relationship)*
A relationship from an object in a domain hierarchy (Company or World) representing a message originator to an object in a domain hierarchy (Company or World) representing a message recipient, together with the associated policy rules.[2] For a subscriber message with multiple recipients, recipients associated with the same applicable message policy rules are grouped into recipient groups.

[2] Application Note: A relationship may be from an object in the Company domain hierarchy to an object in the World domain hierarchy, from an object in the World domain hierarchy to an object in the Company domain hierarchy, from an object in the Company domain hierarchy to an object in the Company domain hierarchy, or from an object in the World domain hierarchy to an object in the World domain hierarchy. In the latter two cases, a relationship may be from an object to itself.
Usually, one set of relationships (either Company to World, or World to Company) is for the expected direction of message flow through the Policy Server, and the other three sets of relationships are used to specify policy for subscriber messages whose originator or recipients do not match the expected direction of message flow. Examples of such messages are:

- legitimate messages after some forms of list expansion or redirection
- the result of inconsistent configuration between message routing and message policy
- for application of message policy to intra-domain messages intentionally routed through the Policy Server
- bogus messages with spoofed originator addresses.

*PKI Configuration Administrator*

This TOE administrator configures, *inter alia*, the PKI data required to identify and authenticate CSDS Server-mode Administrators, CSDS Directory-mode Administrators and X.841 Security (Label) Policy Administrators on Policy Servers, CSDS Directory-mode Administrators on ClearPoint in Directory-mode and X.841 Security (Label) Policy Administrators on SPIF Editors. A PKI Configuration Administrator is identified and authenticated by the IT environment (for a Policy Server, a CSB2 Administrator acting in the 'cots' role associated with the Policy Server authorised to manage PKI data; for ClearPoint, a ClearPoint Management Station Administrator authorised to manage PKI data; for SPIF Editors, a SPIF Editor Platform Administrator authorised to manage PKI data).

*PKI Configuration Utility* The Policy Server component that allows a PKI Configuration Administrator to manage Policy Server PKI data.

*Policy Engine* The Policy Server component that mediates and audits subscriber messages between subscriber networks for the direction of message flow handled by that Policy Server. The Policy Engine component excludes the external libraries.

*Policy Server* One of two instantiations of the set of Policy Server components (including a Policy Engine, Administration Service, Q-handler Service, PKI Configuration Utility, and Directory Synchronisation Agent) 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). The Policy Server component includes all software in the associated CSB2 VET compartment.

*Policy Server Configuration Data*

Policy Server specific configuration data that is defined and modified by a CSDS Server-mode Administrator using ClearPoint in Server-mode. The contents of Policy Server Configuration Data are described in Annex B.

*PROXY compartment** A CSB2 compartment, which is connected to one of the subscriber networks.

*Q-handler Service* The Policy Server component that associates Policy Engine message queues with CSB2 queues in accordance with the direction of subscriber message flow through the Policy Server.

*Recipient group* For a multi-recipient subscriber message, the set of recipients having the same applicable Message Policy rules.

*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.

*Server-mode*
A mode of operation of ClearPoint in which CSDS Server-mode Administrators manage a Policy Server using a ClearPoint Management Station on a DMZ network that is in direct communication with the Administration Service on the Policy Server.

*SPIF Editor*
An optional component of CSDS residing on a Linux or Solaris or Microsoft Windows platform, comprising policy management software with an intuitive GUI interface to define or modify an X.841 Security (Label) Policy Information File (SPIF) and store this in a DSA.

*SPIF Editor Platform*
A component of CSDS, comprising SPIF Editor and external libraries, residing on a suitable hardware platform incorporating a Microsoft Windows, Linux or Solaris OS.

*SPIF Editor Platform Administrator*
An IT Environment Administrator permitted to manage, *inter alia*, SPIF Editor PKI data, who is identified and authenticated by the SPIF Editor Platform, which could be achieved by a variety of means, including use of the Microsoft Windows, Linux or Solaris OS; tokens on attached devices (e.g. smart cards); dedication of the SPIF Editor Platform to a single user.

*Subscriber*
A user that has electronic access to a subscriber network and may submit and receive messages to and from a CSDS Server 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 a CSDS Server from a subscriber for distribution and routing to other subscribers.

*Subscriber network*
One of two networks (designated Company and World) connected to a CSDS Server (via a CSB2 PROXY compartment) such that the CSDS Server mediates all information flows, including subscriber messages, entering and leaving the CSDS Server from and to the networks.

*TOE Administrator*
An authorised administrator of the CSDS TOE.

*User*
A human or IT entity that has an electronic interface with the TOE 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.

*X.841 Security (Label) Policy Administrator*
An optional TOE administrator authorised by a Policy Server to define and modify X.841 SPIFs (using a SPIF Editor and distribution via DSAs).

## 1.7 References

[ACP 145] Combined Communications Electronics Board (CCEB) Allied Communications Publication ACP 145 (2005), *Gateway-to-Gateway Implementation Guide for ACP 123/Stanag 4406 Messaging Services*.

[ANSI X9.52] Triple Data Encryption Algorithm Modes of Operation, American National Standards Institute, ANSI X9.52-1998, 1998

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

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005:
Part 1 Introduction and general model, CCIMB-2005-08-001
Part 2 Security functional requirements, CCIMB-2005-08-002
Part 3 Security assurance requirements, CCIMB-2005-08-003

[CSB2_ST] CS Bastion II Security Target (EAL4), Clearswift, DN11272/5, 29 May 2003

CS Bastion 2.1 Security Target (EAL4), Clearswift, DN11272/6, 3 September 2004

CS Bastion 2.2 Security Target (EAL4), Clearswift, DN11272/7, 4 April 2006

[FIPS Pub 186] Digital Signature Standard (DSS), National Institute of Standards and Technology, FIPS Pub 186, 19 May 1994

[FIPS Pub 197] Advanced Encryption Standard (AES), National Institute of Standards and Technology, FIPS Pub 197, 26 November 2001

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

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

[SMTP-MIME] Internet Mail & Messaging Formats

IETF RFC 2821, *Simple Mail Transfer Protocol*.

IETF RFC 2822, *Internet Message Format*.

IETF RFC 2045, *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*.

IETF RFC 2046, *Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types*.

IETF RFC 2047, *MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text*.

IETF RFC 2048, *Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures*.

IETF RFC 2049, *Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples*.

IETF RFC 1847, *Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted*.

IETF RFC 2156, *MIXER (Mime Internet X.400 Enhanced Relay): Mapping between X.400 and RFC 822/MIME*.

IETF RFC 2157, *Mapping between X.400 and RFC-822/MIME Message Bodies*.

IETF RFC 2164, *Use of an X.500/LDAP directory to support MIXER address mapping*.

IETF RFC 2231, *MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations*.

IETF RFC 2387, *The MIME Multipart/Related Content-type*.

IETF RFC 2480, *Gateways and MIME Security Multiparts*.

IETF RFC 3461, *Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)*.

IETF RFC 3462, *The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages*.

IETF RFC 3463, *Enhanced Mail System Status Codes*.

IETF RFC 3464, *An Extensible Message Format for Delivery Status Notifications*.

IETF RFC 3798, *Message Disposition Notification*.

[STANAG 4406]

NATO C3 Board Information System Sub-Committee STANAG 4406 (Ed.2 -2005), *Military Message Handling System*

[S/MIME] Secure/Multipurpose Internet Mail Extensions

IETF RFC 3851, *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification*.

IETF RFC 3852, *Cryptographic Message Syntax (CMS)*.

IETF RFC 3370, *Cryptographic Message Syntax (CMS) Algorithms*.

IETF RFC 3850, *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling*.

IETF RFC 2634, *Enhanced Security Services for S/MIME*.

IETF RFC 2631, *Diffie-Hellman Key Agreement Method*.

IETF RFC 3447, *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*.

IETF RFC 3565, *Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)*.

IETF RFC 3854, *Securing X.400 Content with Secure/Multipurpose Internet Mail Extensions (S/MIME)*.

IETF RFC 3855, *Transporting Secure/Multipurpose Internet Mail Extensions (S/MIME) Objects in X.400*.

[X.400] Message Handling Systems

ITU-T Recommendation F.400/X.400 (1999) | ISO/IEC 10021-1: 2003, *Information technology - Message Handling Systems (MHS) - System and service overview.*

ITU-T Recommendation X.402 (1999) | ISO/IEC 10021-2: 2003, *Information technology - Message Handling Systems (MHS) - Overall architecture.*

ITU-T Recommendation X.411 (1999) | ISO/IEC 10021-4: 2003, *Information technology - Message Handling Systems (MHS) - Message transfer system: Abstract service definition and procedures.*

ITU-T Recommendation X.413 (1999) | ISO/IEC 10021-5: 1999, *Information technology - Message Handling Systems (MHS) - Message store: Abstract service definition.*

ITU-T Recommendation X.419 (1999) | ISO/IEC 10021-6: 2003, *Information technology - Message Handling Systems (MHS) - Protocol specifications.*

ITU-T Recommendation X.420 (1999) | ISO/IEC 10021-7: 2003, *Information technology - Message Handling Systems (MHS) - Interpersonal messaging system.*

ITU-T Recommendation F.435 (1999) / ISO/IEC 10021-8: 1999, *Information technology - Message Handling Systems (MHS) - Electronic Data Interchange Messaging Service.*

ITU-T Recommendation X.435 (1999) | ISO/IEC 10021-9: 1999, *Information technology - Message Handling Systems (MHS) - Electronic Data Interchange Messaging System.*

ITU-T Recommendation X.412 (1999) | ISO/IEC 10021-10: 1999, *Information technology – Message Handling Systems (MHS) – MHS Routing.*

ITU-T Recommendation X.404 (1999) | ISO/IEC TR 10021-11: 1999, *Information technology – Message Handling Systems (MHS) – MHS Routing: Guide for Messaging System Managers.*

[X.500] Directory Systems

ITU-T Recommendation X.500 (2001) | ISO/IEC 9594-1: 2001, *Information technology – Open Systems Interconnection – The Directory – Overview of concepts, models, and services.*

ITU-T Recommendation X.501 (2001) | ISO/IEC 9594-2: 2001, *Information technology – Open Systems Interconnection – The Directory – Models.*

ITU-T Recommendation X.509 (2000) | ISO/IEC 9594-8: 2001, *Information technology – Open Systems Interconnection – The Directory – Authentication framework.*

ITU-T Recommendation X.511 (2001) | ISO/IEC 9594-3: 2001, *Information technology – Open Systems Interconnection – The Directory – Abstract service definition.*

ITU-T Recommendation X.518 (2001) | ISO/IEC 9594-4: 2001, *Information technology – Open Systems Interconnection – The Directory – Procedures for distributed operation.*

ITU-T Recommendation X.519 (2001) | ISO/IEC 9594-5: 2001, *Information technology – Open Systems Interconnection – The Directory – Protocol specifications.*

ITU-T Recommendation X.520 (2001) | ISO/IEC 9594-6: 2001, *Information technology – Open Systems Interconnection – The Directory – Selected attribute types.*

ITU-T Recommendation X.521 (2001) | ISO/IEC 9594-7: 2001, *Information technology – Open Systems Interconnection – The Directory – Selected object classes.*

ITU-T Recommendation X.525 (2001) | ISO/IEC 9594-9: 2001, *Information technology – Open Systems Interconnection – The Directory – Replication*.

ITU-T Recommendation X.530 (2001) | ISO/IEC 9594-10: 2001, *Information technology – Open Systems Interconnection – The Directory – Use of systems management for administration of the Directory*.

[X.841] ITU-T Recommendation X.841 (2000) | ISO/IEC 15816: 2002, *Information technology – Security techniques – Security information objects for access control*.

# 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 CSDS Overview

Clearswift DeepSecure (CSDS) is a comprehensive email policy 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 active Message Policy, which is determined from attributes of the subscriber message, including its originator and recipients.

CSDS supports a number of administrative roles and administrator privileges that permit authorised administrators to define and modify Message Policy, select and activate a specific Message Policy, manage message queues, configure and view message archives, audit logs, and diagnostic logs, modify X.841 SPIFs and stop/re-start message processing.

A CSDS deployment comprises one or more CSDS Servers, two or more ClearPoint Management Stations, and optionally one or more SPIF Editors.

Each CSDS Server operates independently of any other CSDS Server, although any number of CSDS Servers may be co-located, with Policy Servers associated with the same direction of subscriber message flow being jointly managed. In general, Policy Server management functions must be performed from a ClearPoint Management Station attached to the DMZ network or locally from a CSB2 terminal. However, Message Policy and X.841 SPIFs may be exclusively modified from another network connected to the DMZ network (see Section 2.2 for further detail).

A CSDS Server resides on and interfaces with a single EAL4 certified CSB2/TSOL platform, which provides CSDS with two channels, one for each direction of subscriber 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 the TOE (see Section 2.3 for further detail).

A CSDS Server 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 CSDS Network Environment

As stated in Section 2.1, a CSDS deployment comprises one or more CSDS Servers, two or more ClearPoint Management Stations, and optionally one or more SPIF Editors.

A single CSDS Server is connected to two subscriber networks. One network is designated the ‘Company’ network (generally the network that is part of the organisation that controls the

TOE); 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.

It is assumed that a packet firewall is used to protect the CSDS Server and the CSB2/TSOL platform from denial of service attacks from each subscriber network if it is considered hostile. One or more border MTAs may be used to concentrate subscriber message traffic, or alternatively the PROXY may be configured for direct connection to specific MTAs within the network.

A CSDS Server comprises two Policy Servers, one for each direction of subscriber 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, configuring and viewing audit logs and stop/re-start of the Policy Engine must be performed using the ClearPoint Management Station on the DMZ network in direct communication with the Policy Server (Server-mode). Definition and modification of a Message Policy may also be performed using ClearPoint in Server-mode.

Usually, each DMZ network will contain one or more directory servers (DSAs). A DSA may contain any of:

- X.509 Certificates (authenticating public keys) and Certificate Revocation Lists (CRLs) created by Certification Authorities
- X.841 Security (Label) Policy Information (SPIFs) created by X.841 Security (Label) Policy Administrators (possibly using the DeepSecure SPIF Editor)
- Message Policy defined or modified by CSDS Directory-mode Administrators using ClearPoint in Directory-mode
- Malicious code definition or spam definition updates uploaded using a Directory Synchronisation Uploader.

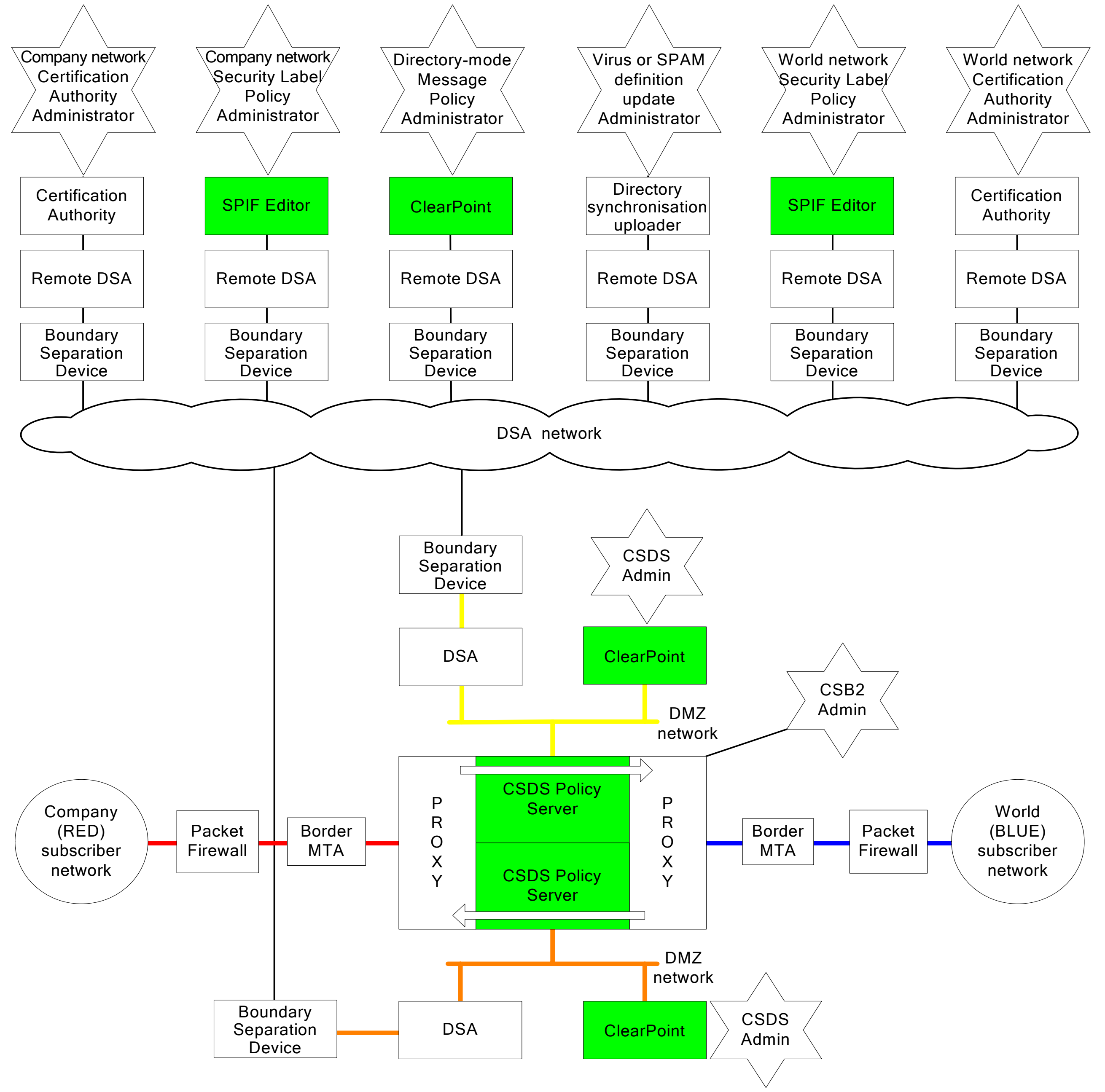
Frequently the data contained in the DSAs on the DMZ network will be replicated copies of data from remote DSAs. Where automatic replication of DSA data is required the DSAs on the DMZ network may be connected to the remote DSAs (or DSA networks) through appropriately assured boundary separation devices.

Each Policy Server must be configured for definition and modification of Message Policy using ClearPoint exclusively in either Server-mode or Directory-mode.

Figure 2.1, Figure 2.2 and Figure 2.3 illustrate some examples of possible CSDS network environment configurations. These examples are intended to illustrate possible configurations, and are not intended to be prescriptive or to limit deployment configurations to only these possibilities. Rather, the examples are provided to suggest possibilities that may be combined as appropriate for each specific deployment. In the examples each management function is shown separately for generality, but this is not intended to preclude co-location of management functions where this is desired.

In figures in this section, the TOE is contained within the green coloured areas. Networks connected to the CSDS Server are shown using CSB2 colour conventions: Red for Company network, Blue for World network, Yellow for the DMZ network associated with the VET compartment managing subscriber messages outgoing from the Company network, and Orange for the DMZ network associated with the VET compartment managing subscriber messages incoming to the Company network.  Remote networks (i.e. those separated by a Boundary Separation Device) are black.

Figure 2.1 shows remote management systems, assumed to be each in a different location, each directly connected to a DSA which is itself connected to a (distributed) network of DSAs through an appropriately assured Boundary Separation Device.  If some remote management systems were in the same location they could share access to a common DSA (not illustrated). Each DMZ network is also connected to this network of DSAs, again through an appropriately assured Boundary Separation Device.  The network of DSAs may contain other Boundary Separation Devices within it (not illustrated) if it spans different security domains.

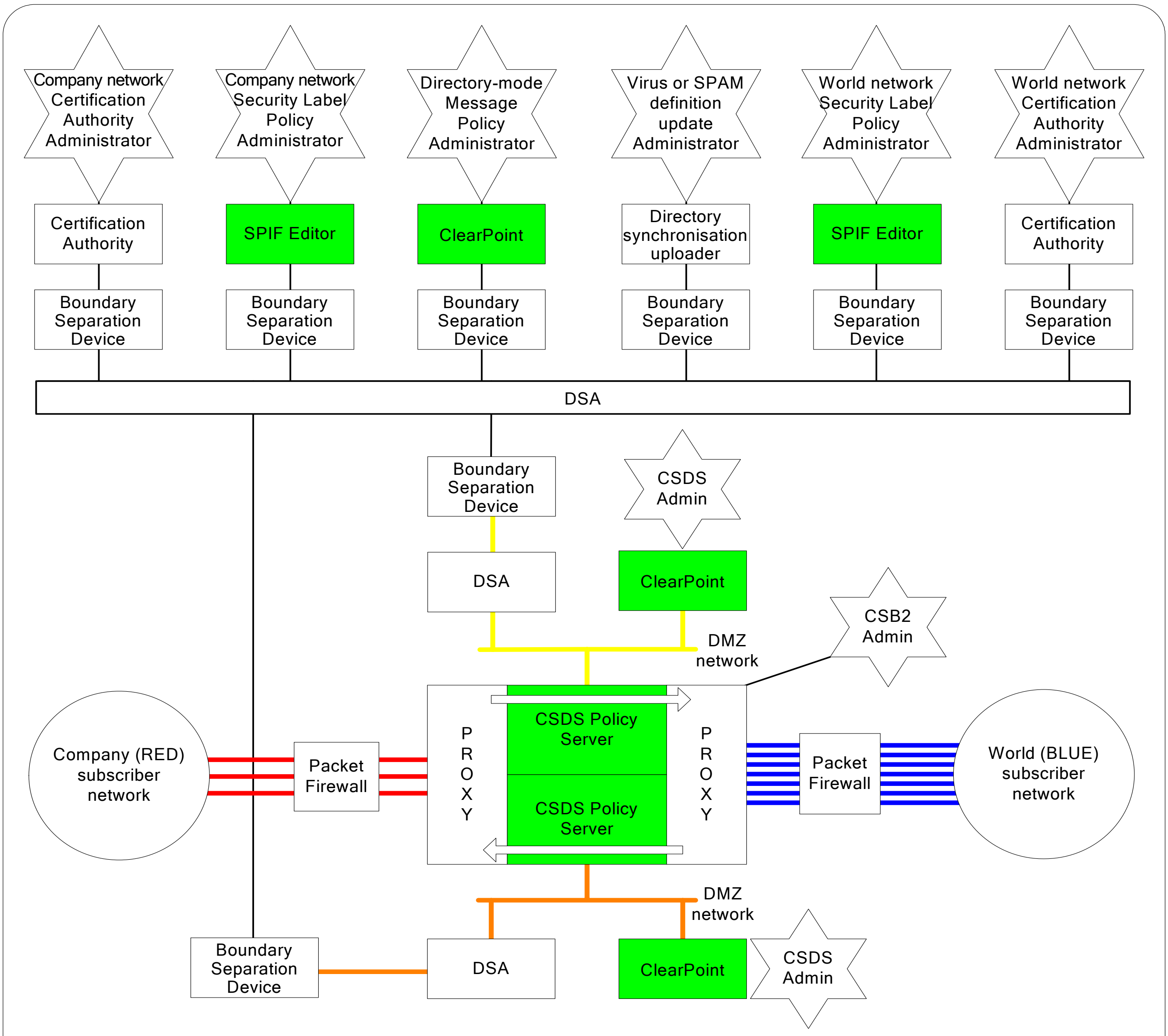

Company network Certification Authority Administrator
Company network Security Label Policy Administrator
Directory-mode Message Policy Administrator
Virus or SPAM definition update Administrator
World network Security Label Policy Administrator
World network Certification Authority Administrator
Certification Authority
SPIF Editor
ClearPoint
Directory synchronisation uploader
SPIF Editor
Certification Authority
Remote DSA
Remote DSA
Remote DSA
Remote DSA
Remote DSA
Remote DSA
Boundary Separation Device
Boundary Separation Device
Boundary Separation Device
Boundary Separation Device
Boundary Separation Device
Boundary Separation Device
DSA network
Boundary Separation Device
CSDS Admin
DSA
ClearPoint
CSB2 Admin
DMZ network
Company (RED) subscriber network
Packet Firewall
Border MTA
PROXY
CSDS Policy Server
CSDS Policy Server
PROXY
Border MTA
Packet Firewall
World (BLUE) subscriber network
DMZ network
Boundary Separation Device
DSA
ClearPoint
CSDS Admin

An example CSDS deployment
(TOE is within coloured areas: CSDS Server, ClearPoint management stations and SPIF Editors)
Also illustrates location of administrators

Figure 2.1 Single CSDS in its assumed environment (Example 1)

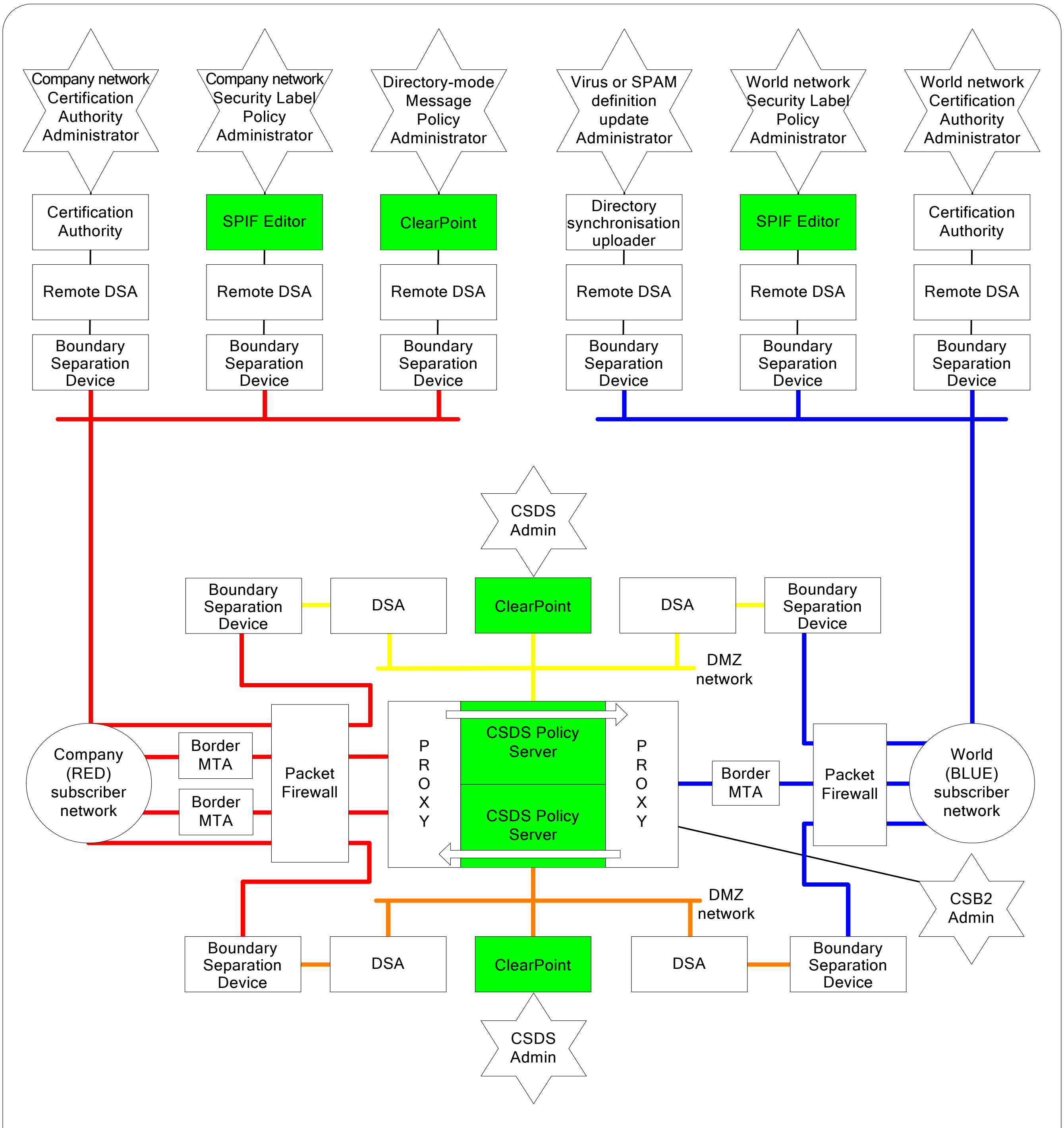
Figure 2.2 shows each remote management system with an appropriately assured Boundary Separation Device between it and the DSA to which it connects. A single common remote DSA is illustrated, although this could equally well be a (distributed) network of DSAs. As this configuration protects the management system but not its communication with its DSA, in this configuration each management system should use Strong Authentication to the DSA, unless the DSA (network) itself is adequately protected.

Figure 2.2 also illustrates each PROXY connecting directly to a number of MTAs in its subscriber network instead of using a border MTA.


Company network Certification Authority Administrator
Company network Security Label Policy Administrator
Directory-mode Message Policy Administrator
Virus or SPAM definition update Administrator
World network Security Label Policy Administrator
World network Certification Authority Administrator
Certification Authority
SPIF Editor
ClearPoint
Directory synchronisation uploader
SPIF Editor
Certification Authority
Boundary Separation Device
Boundary Separation Device
Boundary Separation Device
Boundary Separation Device
Boundary Separation Device
Boundary Separation Device
DSA
Boundary Separation Device
CSDS Admin
DSA
ClearPoint
DMZ network
CSB2 Admin
Company (RED) subscriber network
Packet Firewall
PROXY
CSDS Policy Server
CSDS Policy Server
PROXY
Packet Firewall
World (BLUE) subscriber network
DMZ network
Boundary Separation Device
DSA
ClearPoint
CSDS Admin

An example CSDS deployment
(TOE is within coloured areas: CSDS Server, ClearPoint management stations and SPIF Editors)
Also illustrates location of administrators

Figure 2.2 Single CSDS in its assumed environment (Example 2)


Company network Certification Authority Administrator
Company network Security Label Policy Administrator
Directory-mode Message Policy Administrator
Virus or SPAM definition update Administrator
World network Security Label Policy Administrator
World network Certification Authority Administrator
Certification Authority
SPIF Editor
ClearPoint
Directory synchronisation uploader
SPIF Editor
Certification Authority
Remote DSA
Remote DSA
Remote DSA
Remote DSA
Remote DSA
Remote DSA
Boundary Separation Device
Boundary Separation Device
Boundary Separation Device
Boundary Separation Device
Boundary Separation Device
Boundary Separation Device
CSDS Admin
Boundary Separation Device
DSA
ClearPoint
DSA
Boundary Separation Device
DMZ network
Company (RED) subscriber network
Border MTA
Border MTA
Packet Firewall
PROXY
CSDS Policy Server
CSDS Policy Server
PROXY
Border MTA
Packet Firewall
World (BLUE) subscriber network
CSB2 Admin
DMZ network
Boundary Separation Device
DSA
ClearPoint
DSA
Boundary Separation Device
CSDS Admin

An example CSDS deployment
(TOE is within coloured areas: CSDS Server, ClearPoint management stations and SPIF Editors)
Also illustrates location of administrators

Figure 2.3 Single CSDS in its assumed environment (Example 3)

Figure 2.3 shows remote management systems' DSAs connecting to DSAs on the DMZ network through each subscriber network. It also illustrates other possible configurations of Border MTAs and Packet Firewalls.

Each possible configuration of the remote management elements of the CSDS network environment has the commonality that information managed remotely which affects the operation of CSDS is digitally signed by the relevant administrator when it is defined or modified, uploaded by the remote management software into a remote DSA, replicated from the remote DSA into a DSA on each DMZ network (either using automatic Directory replication, or manual equivalent), and that the Policy Server validates the digital signature to ensure integrity and authenticity to a configured authorised remote administrator before making use of such information.

It is assumed that the DMZ and remote management networks, including CSDS Server, ClearPoint Management Stations, SPIF Editor Platforms and the CSB2/TSOL platform, are protected from attacks from connecting networks by appropriately assured boundary separation devices (e.g. a packet firewall and application level firewall). Appropriate assurance for the boundary separation device would depend on the nature of the connecting 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, manage message queues, configure and view audit logs and stop/re-start the Policy Engine
- message modification or eavesdropping attacks
- denial of service attacks.

As stated in Section 2.1, each CSDS Server operates independently of any other CSDS Server, although any number of CSDS Servers may be co-located and jointly managed. Co-located and jointly managed instances of CSDS are referred to as a Policy Server farm (see Figure 2.4 and Figure 2.5 for two example configurations). In a CSDS Policy Server farm it is assumed that each of the Policy Servers on different CSDS Servers that are controlling subscriber 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 subscriber message flow in the other direction.

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.

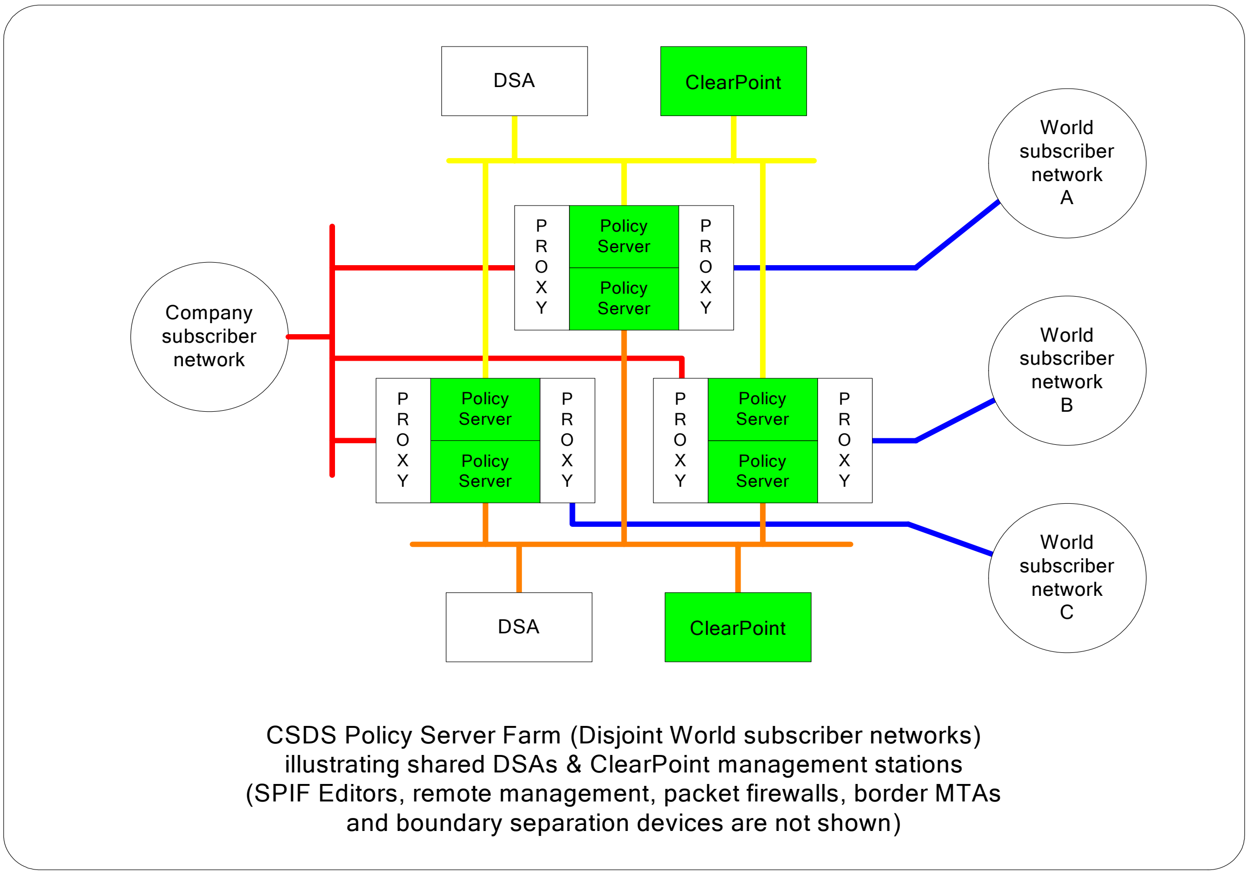

DSA
ClearPoint
World subscriber network A
P R O X Y
Policy Server
Policy Server
P R O X Y
Company subscriber network
World subscriber network B
P R O X Y
Policy Server
Policy Server
P R O X Y
P R O X Y
Policy Server
Policy Server
P R O X Y
World subscriber network C
DSA
ClearPoint
CSDS Policy Server Farm (Disjoint World subscriber networks)
illustrating shared DSAs & ClearPoint management stations
(SPIF Editors, remote management, packet firewalls, border MTAs
and boundary separation devices are not shown)

Figure 2.4 CSDS Policy Server Farm (Example 1)

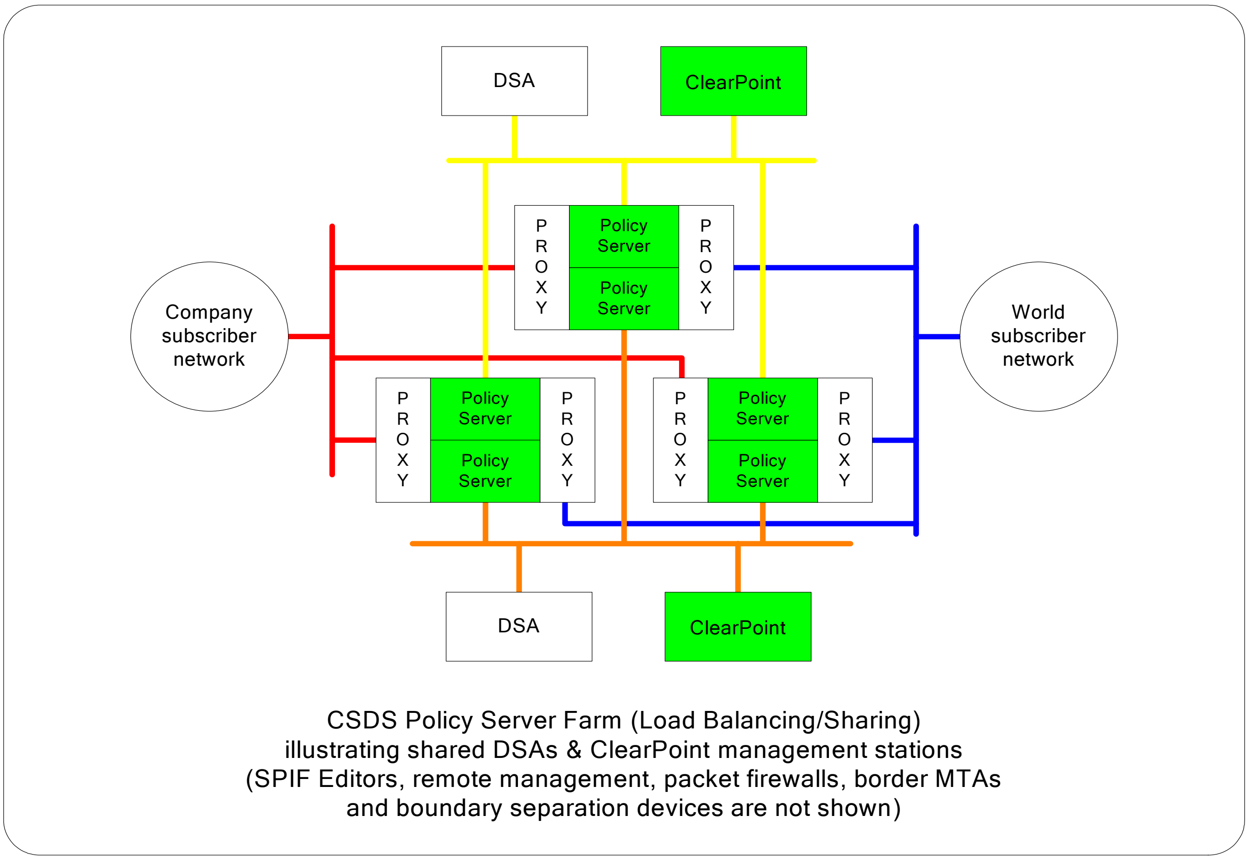

DSA
ClearPoint
PROXY
Policy Server
Policy Server
PROXY
Company subscriber network
World subscriber network
PROXY
Policy Server
Policy Server
PROXY
PROXY
Policy Server
Policy Server
PROXY
DSA
ClearPoint
CSDS Policy Server Farm (Load Balancing/Sharing)
illustrating shared DSAs & ClearPoint management stations
(SPIF Editors, remote management, packet firewalls, border MTAs
and boundary separation devices are not shown)

Figure 2.5 CSDS Policy Server Farm (Example 2)

## 2.3 CSB2/TSOL Platform

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

As stated in Section 2.1, a CSDS Server resides on and interfaces with a single EAL4 certified CSB2/TSOL platform, which provides the CSDS Server with two channels, one for each direction of subscriber 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 or assurance maintained configurations of CSB2 (see [CSB2_ST]). The CSB2 optional DMZ (ARCHIVE) compartment is not used in CSDS – CSDS subscriber 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 certificate trust points.

## 2.4 CSDS Components

As stated in Section 2.1, a CSDS deployment comprises one or more CSDS Servers, two or more ClearPoint Management Stations, and optionally one or more SPIF Editors.

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

A Policy Server comprises the following components:

- Policy Engine
- External Libraries
- Q-handler Service
- Administration Service
- Directory Synchronisation Agent
- PKI Configuration Utility.

A ClearPoint Management Station comprises the following components:

- ClearPoint
- External Libraries.

A SPIF Editor Platform comprises the following components:

- SPIF Editor
- External Libraries.

The SPIF Editor is an optional component that provides configuration used by the X.841 LSL, which is an optional External Library for the Policy Server and ClearPoint Management Station.

These components are described in detail in the following subsections.

The major components and data flows within a CSDS Server are illustrated in Figure 2.6. The Q-handler Service component is not shown, but the various queues are. The PKI Configuration Utility is not shown.

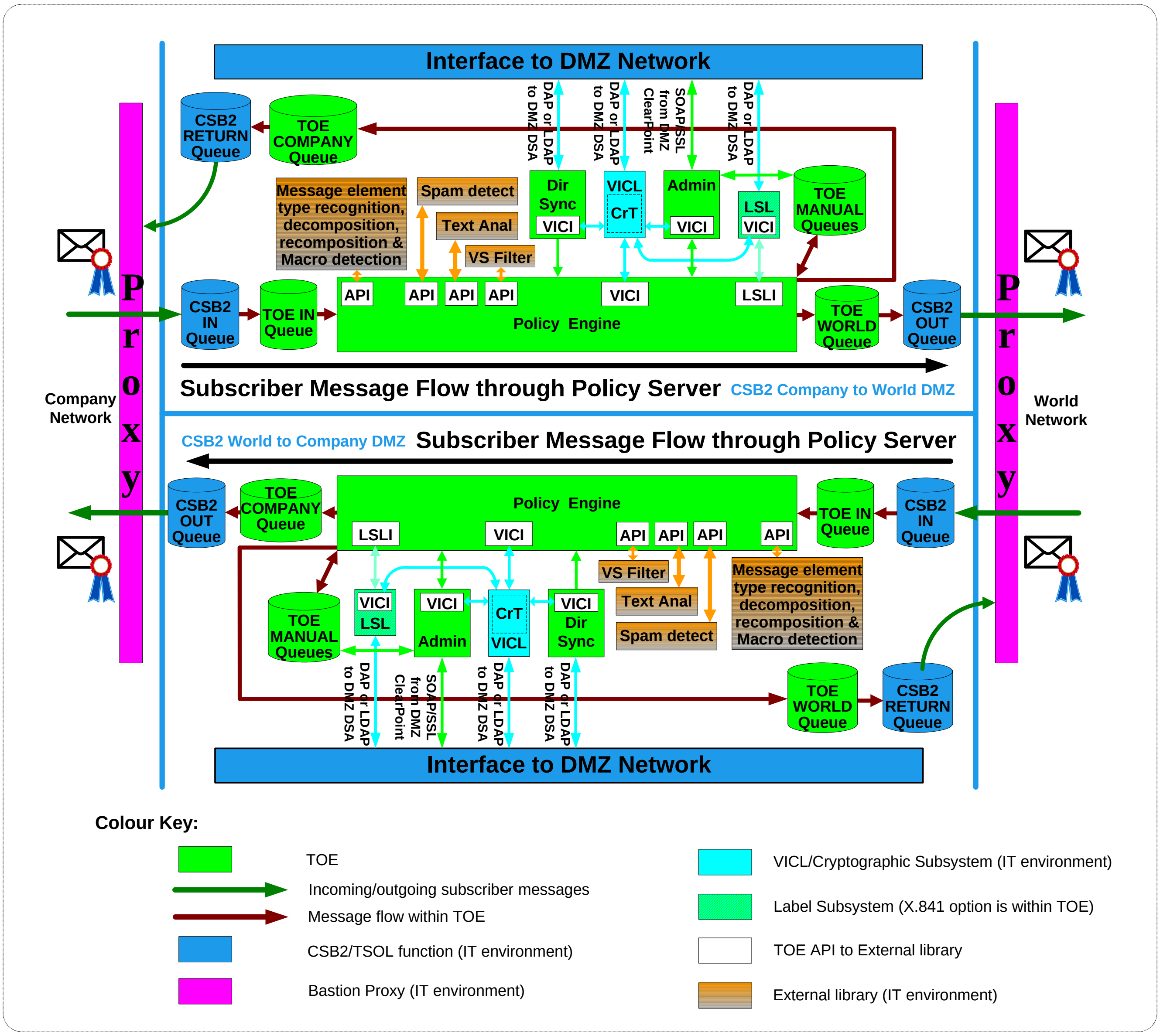


Figure 2.6 CSDS Server

### 2.4.1 Policy Engine

The Policy Engine is responsible for managing and auditing the flow of subscriber messages between subscriber networks, and for the invocation of appropriate rules (checks and actions), in accordance with the active Message Policy. Message security labels may be extracted in accordance with proprietary standards for informal (text) labels, or with [RFC 2634] and [STANAG 4406] and [X.411] for formal (binary-encoded) labels. 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.

Each subscriber message may have one or more recipients, at least one originator and, where more than one signature is present, more than one originator.

Message Policy consists of sets of policy rules and attribute settings between pairs of objects (originator/recipient pairs), where each object is in a hierarchy with either Company domain or World domain 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 (See Annex A for a description of the contents of a Message Policy).

Each Policy Server may contain any number of Message Policies. 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. The Policy Engine checks that the active Message Policy is valid (i.e. it is a compatible version, and it complies with the schema) as it starts. There is no flow of subscriber messages through a Policy Server unless the Policy Engine is loaded with a valid 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.

The following baseline checks are enforced by the Policy Engine (excluding those parts performed by external libraries):

- Ensure that all subscriber messages conform to the SMTP and X.400 messaging protocols, as defined in the relevant [SMTP-MIME], [S/MIME], [STANAG 4406] and [X.400] standards
- Identify the originator/recipient pairs in a subscriber message and ensure they fall within the Domains defined by the active Message Policy
- Checks for authorised X.400 message types (Delivery Reports, Receipt Notifications and Probes)
- Checks for authorised SMTP message types (Delivery Status Notifications, Message Disposition Notifications)
- Checks for authorised STANAG 4406 Precedence and X.400 Priority
- Checks for authorised X.400 content types and body-part types
- Checks for authorised SMTP headers
- Check subscriber message size against Message Policy defined maxima
- PKI state checks (using cryptographic operations from the external VIC library)
- Security Label checks in formal security label (using security label comparison, mapping and rendering functions provided by the external LSL)
- Security Label checks in first line of text
- Security Label checks in Subject heading field

The following baseline actions are enforced by the Policy Engine (excluding those parts performed by external libraries):

- Modify specific message fields
- Security label conversion of formal security label (using security label mapping and rendering functions provided by the external LSL)
- PKI state conversions (using cryptographic operations from the external VIC library)
- Primary actions of subscriber message: pass-through (to recipient); queue for manual intervention, delete with notification (non-deliver) and delete silently (discard)
- Subscriber message release, non-delivery or discard from MANUAL queues after manual intervention
- Archive a subscriber message, as it enters and/or as it leaves a Policy Engine

- Audit subscriber message transactions
- Add textual annotations to a subscriber message
- Remove or replace subscriber message parts
- Send non-delivery reports
- Send notification messages.

Incoming subscriber messages enter the Policy Engine via its IN queue and successfully mediated subscriber 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). Subscriber messages that fail mediation may be non-delivered or placed in a MANUAL queue (to be held for examination, action and possible release, non-delivery or discard by CSDS Server-mode Administrators having the Queue Management administrator privilege).

The Policy Engine processes higher precedence subscriber messages before queued subscriber messages of lower precedence, can apply maximum subscriber message transit time limits, and can generate warning messages to administrators if operational thresholds are exceeded.

### 2.4.2 External Libraries

The following external libraries may be invoked by the Policy Engine to perform the additional checks and actions, and those parts of the Policy Engine checks and actions that are excluded from the Policy Engine:

- data type recognition, decomposition, text extraction, macro detection and re-composition
- textual analysis subsystem
- Virus Scanner (VS) subsystem
- spam detection subsystem
- formal security label subsystem
- cryptographic subsystem.

The cryptographic subsystem is also used by the Administration Service, the Directory Synchronisation Agent, the PKI Configuration Utility, the X.841 option for the formal security label subsystem, ClearPoint and the SPIF Editor.

The TOE ensures that cryptographic operations are handled correctly by invoking the cryptographic subsystem via a Vendor Independent Cryptographic API (VICI). The cryptographic subsystem communicates with a DSA on the DMZ network via DAP or LDAP to access, for example, public key certificates and certificate revocation lists.

The formal security label subsystem is also used by ClearPoint.

The TOE ensures that formal security label checking operations are handled correctly by invoking the formal security label subsystem via a Label Support Library API (LSLI). The X.841 formal security label subsystem communicates with a DSA on the DMZ network via the VICI to access SPIFs, and uses VICI to authenticate and validate the integrity of SPIFs.

### 2.4.3 Q-handler Service

The Q-handler Service is responsible for the association of Policy Engine queues with CSB2 queues in accordance with the direction of subscriber message flow through the Policy Server. The Policy Engine IN queue is always associated with the CSB2 IN queue.

If the direction of subscriber 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 subscriber 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.

### 2.4.4 Administration Service

The Administration Service supports administration, using ClearPoint in Server-mode, of the Message Policy and Policy Engine queues, archives, audit logs and diagnostic logs by authorised CSDS Server-mode Administrators acting with one or more of the following administrator privileges:

- Message Policy Administration, which permits definition and modification of the behaviour of a Message Policy that is stored on a Policy Server, as well as viewing of a Message Policy
- Message Policy Selection, which permits selection and activation of a Message Policy, as well as viewing of a Message Policy and stop/start of a Policy Engine
- Message Policy Viewing, which permits viewing of a Message Policy
- Policy Server Configuration Administration, which permits configuration of message archives, audit logs, and other Policy Server attributes, as well as viewing of Policy Server attributes and stop/start of a Policy Engine
- Policy Server Configuration Viewing, which permits viewing of Policy Server attributes
- Queue Management, which permits message release, non-delivery or discard actions on subscriber messages in MANUAL queues, as well as viewing of the status of message queues
- Queue Viewing, which permits viewing of the status of message queues
- Archive Viewing, which permits searching for and viewing of subscriber messages in archives
- Audit Log Viewing, which permits viewing of the contents of audit logs
- Diagnostic Log Configuration, which permits configuration and viewing of diagnostic logs and stop/start of a Policy Engine.

CSDS Server-mode Administrators, and their authorised administrator privileges, are identified and authenticated by validation of individual X.509 certificates via the cryptographic subsystem invoked through VICI.

The Administration Service records the following audit events:

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

### 2.4.5 Directory Synchronisation Agent

The Directory Synchronisation Agent supports administration, using ClearPoint in Directory-mode, of the Message Policy by authorised CSDS Directory-mode Administrators, who are permitted to define and modify the behaviour of a Message Policy that is stored in a DSA.

The integrity of each Message Policy transferred from a ClearPoint Management Station to a DSA, between DSAs in a DSA network, to a DSA on the DMZ network and thence to the Policy Server, is protected by a digital signature, which is applied by the ClearPoint Management

Station and verified by the Directory Synchronisation Agent using VICI (and thus the cryptographic subsystem).

CSDS Directory-mode Administrators are identified and authenticated using X.509 certificates via the cryptographic functions invoked through VICI.

The Directory Synchronisation Agent also supports administration of malicious code definition and spam definition updates stored in a DSA by IT Environment administrators using a Directory Synchronisation Uploader.

The integrity of each malicious code definition and spam definition update transferred from a Directory Synchronisation Uploader to a DSA, between DSAs in a DSA network, to a DSA on the DMZ network and thence to the Policy Server, is protected by a digital signature, which is applied by the Directory Synchronisation Uploader and verified by the Directory Synchronisation Agent using VICI (and thus the cryptographic subsystem).

The Directory Synchronisation Agent records the following audit events:

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

### 2.4.6 PKI Configuration Utility

CSDS also provides a PKI Configuration Utility, which is used by a PKI Configuration Administrator to support the correct configuration of PKI data (crypto tokens containing private keys, certificate trust points, CSDS Server-mode Administrators' certificates with permitted administrator privileges, CSDS Directory-mode Administrators' certificates, SPIF administrators' certificates, and parameters for communicating with DSAs and maintaining caches of data retrieved from DSAs) loaded into a Policy Server.

The PKI Configuration Utility records the following audit events:

- Changes to PKI data.

### 2.4.7 ClearPoint Management Station

A ClearPoint Management Station provides CSDS Server-mode Administrators and CSDS Directory-mode Administrators with ClearPoint, comprising an intuitive Graphical User Interface (GUI), to define and modify the behaviour of a Message Policy and perform other management functions. ClearPoint resides on a suitable Microsoft Windows workstation (see Section 2.7.2).

The ClearPoint GUI provides four broad functions:

(1) Configuration of PKI attributes (required to access DSA)
(2) Definition and modification of Message Policies
(3) Policy Server configuration (e.g. audit roll-over periods, default log-levels, administrator email identities)
(4) Run-time management of Policy Servers (e.g. stop/re-start Policy Engine, select Message Policy, queue-management, viewing audit logs).

ClearPoint operates in one of two distinct modes (selectable from the initial ClearPoint 'welcome' screen):

- Server-mode
- Directory-mode.

In Server-mode ClearPoint connects direct to a Policy Server (over SOAP). To operate in this mode the ClearPoint Management Station must reside on the DMZ network. In this mode ClearPoint offers GUI functions (2), (3) and (4) appropriate to the administrator privileges of the CSDS Server-mode Administrators.

In Directory-mode ClearPoint connects to a DSA (over DAP or LDAP). The DSA and the ClearPoint Management Station may be on the DMZ network, or a connected network. If on a connected network, the DSA stores the master copy of the Message Policy and replicates this Message Policy to a DSA on the DMZ network, which may be via other DSAs or a DSA network. In this mode ClearPoint has no direct access to a Policy Server, so only offers GUI functions (1) and (2).

The integrity of each Message Policy uploaded by ClearPoint to a DSA is protected by a digital signature, which is applied by ClearPoint using VICI and verified using VICI in the receiving system (which may be a Policy Server or another ClearPoint Management Station). CSDS Directory-mode Administrators are also identified and authenticated by this digital signature.

For any given Policy Server, definition and modification of Message Policies is performed using ClearPoint exclusively in Server-mode, or exclusively in Directory-mode.

A ClearPoint Management Station also includes ClearPoint external libraries, which are used to:

- enable management of those parts of Message Policy that are enforced on a Policy Server by Policy Server external libraries
- support ClearPoint management functions (the cryptographic subsystem and formal security label subsystem, as listed in Section 2.4.2).

Direct Communication between ClearPoint on a ClearPoint Management Station on the DMZ network and the Policy Server Administration Service is via the SOAP/XML protocols over HTTP over SSL. ClearPoint SSL uses the Microsoft CryptoAPI (CAPI) and, by default, the CAPI library in Windows. The Administration Service uses VICI (and hence the cryptographic subsystem) to validate the CSDS Server-mode Administrator's certificate used in SSL authentication and thus to establish the permitted administrator privileges for that administrator.

Communication between ClearPoint and a DSA is through VICI and via DAP or LDAP. VICI can be configured to use DAP Strong Authentication when communicating with a DSA that supports this.

Strong Authentication mitigates a potential Denial of Service attack via a DSA where replay of simple authentication allows an impostor to substitute a bogus Message Policy in place of a real one: in this attack the bogus Message Policy will not be used because its digital signature fails verification and the Policy Engine will continue using the previous version, but the loss of the real Message Policy may disrupt future updates to that Message Policy. A variant of this attack where the impostor just deletes the Message Policy from the DSA has a more severe impact, because that Message Policy is consequently deleted at the Policy Server; if the active Message Policy is deleted the Policy Engine uses a memory cache copy of the active Message Policy only until it is next re-started.

### 2.4.8 SPIF Editor & X.841 LSL

An optional component of CSDS residing on a Linux or Solaris or Microsoft Windows platform (see Section 2.7.2), SPIF Editor comprises policy management software with an intuitive GUI interface, which allows an X.841 Security (Label) Policy Administrator to define or modify an X.841 Security (Label) Policy Information File (SPIF) and store this in a DSA.

A SPIF defines a Security Policy (as specified in [X.841]) containing values of the components contained in a formal Security Label (as specified in [X.411] and [RFC 2634]), including the syntax and semantics of Security Categories, to enable values of Security Labels to be compared to a Clearance. A SPIF may also define the rendering of values of components of Security Labels and Clearances into text. Finally, a SPIF may define mappings from values of Security Labels defined by its Security Policy to equivalent values of Security Labels in other Security Policies.

When the X.841 LSL external library option is installed in a Policy Server, the Policy Engine uses the X.841 LSL as required by the appropriate originator/recipient relationship in its active Message Policy to:

- compare each formal Security Label in the subscriber message with the specified Clearance
- map each formal Security Label in the subscriber message into the specified Security Policy
- render formal Security Label parameters into text as necessary for log entries and use in annotations and notification messages.

When configured to use the X.841 LSL external library option, ClearPoint uses the X.841 LSL in order to render Clearance and Security Label parameters for each Security Policy (SPIF) in ClearPoint's Message Policy management GUI and for each message from a Policy Server queue that ClearPoint displays.

The DSA used by the SPIF Editor to store the SPIF may be on the DMZ network, but more usually on a connected network. If on a connected network, the DSA stores the master copy of the SPIF and for each Policy Server that requires this SPIF, replicates the SPIF to a DSA on the DMZ network, which may be via other DSAs or a DSA network. The SPIF is then downloaded by the X.841 LSL onto the Policy Server. The SPIF may also be replicated by other DSAs or a DSA network for downloading to ClearPoint and other SPIF Editors.

The integrity of each SPIF uploaded by a SPIF Editor to a DSA is protected by a digital signature, which is applied by the SPIF Editor using VICI and verified by the X.841 LSL using VICI in the receiving system (which may be a Policy Server, or a ClearPoint Management Station), or verified by using VICI in another SPIF Editor. X.841 Security (Label) Policy Administrators are also identified and authenticated by this digital signature. An audit event is recorded for each SPIF downloaded by the X.841 LSL.

Communication between the SPIF Editor and a DSA is through VICI and via DAP or LDAP.

The SPIF Editor can be configured to use DAP Strong Authentication when communicating with a DSA that supports this. This mitigates a potential Denial of Service attack via a DSA where replay of simple authentication allows an impostor to substitute a bogus SPIF in place of a real one: in this attack the bogus SPIF will not be used because its digital signature fails verification, but the loss of the real SPIF prevents operation of services that depend on access to that SPIF. Such attack is also countered to an extent by the CSDS X.841 LSL which will continue using a memory-cached copy if a subsequent version of that SPIF fails signature verification; however, re-starting the Policy Engine flushes the memory cache. The variant of this attack where the impostor just deletes the SPIF from the DSA has an identical effect.

## 2.5 Logical TOE Description

This section identifies those CSDS functions that are part of the TOE, which fall into the following areas (detailed in following subsections):

- ClearPoint GUI management functions
- SPIF Editor functions (provided when the X.841 SPIF Editor option is included)

- Policy Server functions.

CSDS functions that are not part of the TOE include:

- ClearPoint functions provided by external libraries, including:
    - Cryptographic operations
    - Formal security label operations (other than those provided by the X.841 LSL option)
    - Management functions that enable configuration of Policy Server external libraries used for Message Policy enforcement
- SPIF Editor functions provided by external libraries, including:
    - Cryptographic operations
- Policy Server functions provided by external libraries, including:
    - Decomposition, text extraction, and re-composition of various data types
    - Cryptographic operations
    - Formal security label operations (other than those provided by the X.841 LSL option)
    - The application of mediation checks applied to subscriber message elements for:
        - data type recognition and conformance
        - textual analysis
        - virus scanning
        - macro detection
        - spam detection.

### 2.5.1 ClearPoint GUI management functions

ClearPoint GUI management functions that are part of the TOE include:

- Management of ClearPoint PKI data
- Definition and modification of Policy Server configuration data
- Definition and modification of Domains, Groups and Users (subscribers)
- Definition of originator/recipient pairings (relationships)
- Definition and modification of Message Policy rules and attributes
- Selection and activation of a Message Policy
- Stop/re-start of a Policy Engine
- Execution of queue management functions
- Viewing message archives
- Configuring and viewing Policy Server audit logs
- Configuring and viewing Policy Server diagnostic logs.

### 2.5.2 SPIF Editor functions

SPIF Editor functions that are part of the TOE include:

- Management of SPIF Editor PKI data
- Definition and modification of X.841 SPIFs.

### 2.5.3 Policy Server functions

Policy Server functions that are part of the TOE include:

- Management of Policy Server PKI data
- Association of Policy Engine message queues with CSB2 queues
- Identification and authentication of TOE Administrators (except PKI Configuration Administrators who are identified and authenticated by the IT Environment) and their

permitted roles and administrator privileges (excluding cryptographic operations provided by an external library)

- Download of new or modified Message Policies initiated from ClearPoint in Server-mode by CSDS Server-mode Administrators having Message Policy Administration administrator privilege
- Selection and activation of Message Policies by CSDS Server-mode Administrators having Message Policy Selection administrator privilege
- Viewing of Message Policies by CSDS Server-mode Administrators having one or more of Message Policy Administration, Message Policy Selection or Message Policy Viewing administrator privilege
- Configuration of message archives, audit logs and other Policy Server attributes by CSDS Server-mode Administrators having Policy Server Configuration Administration administrator privilege
- Viewing of Policy Server attributes by CSDS Server-mode Administrators having one or more of Policy Server Configuration Administration or Policy Server Configuration Viewing administrator privilege
- Message release, non-delivery or discard actions on subscriber messages in MANUAL queues by CSDS Server-mode Administrators having Queue Management administrator privilege
- Viewing the status of message queues by CSDS Server-mode Administrators having one or more of Queue Management or Queue Viewing administrator privilege
- Searching for and viewing of subscriber messages in archives by CSDS Server-mode Administrators having Archive Viewing administrator privilege
- Viewing the contents of audit logs by CSDS Server-mode Administrators having Audit Log Viewing administrator privilege
- Configuration and viewing of diagnostic logs by CSDS Server-mode Administrators having Diagnostic Log Configuration administrator privilege
- Stop/start of a Policy Engine by CSDS Server-mode Administrators having one or more of Message Policy Selection, Policy Server Configuration Administration or Diagnostic Log Configuration administrator privilege
- Synchronisation of Message Policies on Policy Servers with those on a DSA on the DMZ network, which have been defined or modified from ClearPoint in Directory-mode by CSDS Directory-mode Administrators
- Synchronisation of SPIFs on Policy Servers with those on a DSA on the DMZ network, which have been defined or modified from a SPIF Editor by X.841 Security (Label) Policy Administrators
- Auditing of authentication attempts, changes to Message Policies and SPIFs, and other events initiated by TOE Administrators
- Formal security label operations provided by the X.841 LSL optional external library
- Policy Engine subscriber message mediation functions detailed below:

  Checks:

  - o Ensure no flow of subscriber messages unless a Message Policy is activated
  - o Correct unpacking of subscriber messages into message elements, and reassembly of message elements into output messages, including parsing as a valid protocol in conformance with relevant [SMTP-MIME], [S/MIME], [STANAG 4406] and [X.400] standards

- Accurate identification and validation of all originator/recipient pairings (relationships) per subscriber message – a valid pairing must fall within the domains defined by, and controlled by, current active Message Policy
- Invocation of all necessary Message Policy mediation checks and actions (on the subscriber message and message elements derived from preliminary subscriber message unpacking) in accordance with per-relationship Message Policy requirements
- Correct invocation of external libraries
- Checks for X.400 message types (Delivery Reports, Receipt Notifications and Probes)
- Checks for SMTP message types (Delivery Status Notifications, Message Disposition Notifications)
- Checks for STANAG 4406 Precedence and X.400 Priority
- Checks for X.400 content-type and body-part type in message elements
- Checks for SMTP headers
- Checks for MIME media types
- Subscriber message size checks
- PKI state checks (excluding cryptographic operations provided by an external library)
- Checks of formal security labels (excluding formal security label operations provided by an external library)
- Checks of informal text security labels in first line of text
- Checks of informal text security labels in Subject heading field

Actions:

- Modify specific message fields
- Conversions of formal security labels (excluding formal security label operations provided by an external library)
- PKI state conversions (excluding cryptographic operations provided by an external library)
- Processing higher precedence subscriber messages before queued subscriber messages of lower precedence
- Application of maximum subscriber message transit time limits
- Generation of warning messages to administrators if operational thresholds are exceeded
- Subscriber message pass-through, non-delivery, discard or queuing for manual inspection in MANUAL queues
- Release, non-delivery or discard of subscriber messages from MANUAL queues in accordance with manual inspection directives
- Accurate routing and delivery of messages, including internally generated notifications, to the correct subscriber network interface
- Logging of associated audit records
- Actions to generate inbound or outbound archives
- Actions to remove or replace subscriber message elements
- Actions to annotate subscriber messages
- Actions to generate notification messages and non-delivery reports.

## 2.6 Physical TOE Description

Physically the TOE comprises those CSDS product components that provide the logical functionality specified in the above section:

- The Policy Server (excluding external libraries – see below)
- ClearPoint (excluding external libraries – see below)
- The X.841 LSL option
- The X.841 SPIF Editor option.

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

- The Policy Server external libraries for:
  - data type recognition, decomposition, text extraction, macro detection and re-composition
  - textual analysis
  - virus scanning
  - spam detection
  - cryptographic operations
  - formal security label operations (other than the X.841 LSL option which is within the TOE)
- The ClearPoint external libraries for:
  - configuring functionality provided through the Policy Engine exclusively by the above Policy Server external libraries excluded from the TOE
  - cryptography
  - formal security labels (other than the X.841 LSL option which is within the TOE)
- The SPIF Editor external libraries for:
  - cryptography
- The encompassing system environments:
  - CSB2/TSOL platform for CSDS Server (including SMTP or X.400 proxies)
  - Internet Explorer on Microsoft Windows workstation for ClearPoint
  - A JAVA VM on Microsoft Windows, Linux or Solaris for the SPIF Editor
- Certification Authority software to create X.509 Certificates and Certificate Revocation Lists
- The CSDS Directory Synchronisation Uploader for uploading malicious code definition and spam definition updates into a remote DSA
- DSAs
- Border MTAs
- Boundary Separation devices
- Packet firewalls.

## 2.7 Evaluated Configurations

The target of the evaluation (TOE) consists of the following software components:

1. CSDS2.1 Policy Servers for CSB2: Policy Engine Vn 5.1.0.65 (Package Vn 3.20.52)
2. CSDS2.1 X.841 Label support library for Solaris: Vn 2.3.0 (Package Vn 3.20.50)
3. CSDS2.1 ClearPoint for Windows: Vn 5.1.40.0
4. CSDS2.1 X.841 Label support library for Windows: Vn 2.3.0
5. CSDS2.1 SPIF Editor for Java platforms: Vn 1.08

Software components 1 & 2 are standard Solaris packages, designed to install on top of TSOL8 and CSB2. Software components 3 & 4 form part of[3] a single self-installing windows executable[4], designed to install on top of a pre-installed Windows server. Software component 5 forms part of[5] a single platform-independent package[4] designed to install on top of a pre-installed Solaris, Windows or Linux server.

Note that all software components listed above are dependent on supporting hardware and OS. The hardware and OS in each case form part of the IT Environment and is discussed in more detail below.

All five components are combined onto appropriate media (e.g. one or more tailored CDs or DVDs) for distribution to CSDS2.1 installation staff and end-customers. Additional IT environment components may be bundled on the same media.

### 2.7.1 Evaluated configuration – external library considerations

Other than suitable hardware and OS, software components 1, 3 and 5 listed above each require a number of supporting external libraries to operate correctly; these libraries also form part of the IT environment. Table 2.1 lists the number of external libraries (by type) that are encompassed within the scope of evaluated configuration.

Table 2.1 Number of external libraries allowed with each component

| Software Component | Supporting external libraries required | | | | | |
|---|---|---|---|---|---|---|
| | VIC | LSL[6] | DataType recognition | Textual analysis | Virus scanner | Spam detection |
| Policy Server | 1 | 1 | Zero or more[7] | Zero or more[7] | Zero or more[7] | Zero or more[7] |
| ClearPoint | 1 | 1 | Zero or more[8] | Zero or more[8] | Zero or more[8] | Zero or more[8] |
| SPIF Editor | 1 | — | — | — | — | — |

Table 2.2 lists the versions of each of the above external libraries that have been selected for inclusion in the CSDS evaluated test configuration. Each listed library will be tested in conjunction with all applicable TOE systems on all applicable platforms. Rationales for alternative versions of each type of library, along with rationales to cover the various possible permutations of libraries are provided in Annex C onwards.

[3] Some Clearswift developed IT-environment components may be bundled into the same self-installing executable.

[4] Industry standard software packaging tools will be used.

[5] SUN's *J2SE Runtime Environment Version 1.4.2 (JRE 1.4.2)* along with some Clearswift developed IT-environment components may be bundled into the same installable package.

[6] Only required if the X.841 LSL module is not part of the deployment.

[7] Limited only by resource constraints.

[8] There is usually one ClearPoint external library corresponding to each Policy Server external library.

Table 2.2 Versions of external libraries in CSDS evaluated test configuration

| External library | Description | Title | Version |
|---|---|---|---|
| VIC | Cryptographic subsystem | Cryptomathic PrimeInk Premium VIC for CSDS | Vn 2.3.0 |
| | | SFL VIC for CSDS | Vn 2.3.0 |
| | | Null VIC for CSDS | Vn 2.3.0 |
| LSL[9] | Formal security label subsystem | Null LSL for CSDS | Vn 2.3.0 |
| DataType recognition | Data-type recognition subsystem on Policy Server together with corresponding ClearPoint external management subsystem | FileID file identifier for CSDS | Vn 1.0.0 |
| | | Magic file identifier for CSDS | Vn 1.0.0 |
| | | Encoded file unencoder for CSDS | Vn 1.0.0 |
| Textual analysis | Textual analysis subsystem on Policy Server together with corresponding ClearPoint external management subsystem | dtSearch lexical analysis for CSDS | Vn 1.0.0 |
| | | Language type lexical analysis for CSDS | Vn 0.1.0 |
| Virus scanner | Virus Scanner subsystem on Policy Server together with corresponding ClearPoint external management subsystem | Sophos virus scanner for CSDS with<br>Sophos SAVI VS for Solaris | Vn 1.0.0<br>Issue March 2006 |
| | | Sophos virus scanner for CSDS with<br>Sophos SAVI VS for Solaris | Vn 1.0.0<br>Issue May 2006 |
| | | Command line virus scanner for CSDS with ClamAV command line scanner for Solaris | Vn 1.0.0<br>Vn 0.88 |
| Spam detection | Spam detection subsystem on Policy Server together with corresponding ClearPoint external management subsystem | SpamAssassin spam scanner for CSDS | Vn 0.1.0 |
| | | SD spam scanner for CSDS | Vn 0.1.0 |

[9] This table excludes the X.841 LSL library because this is a TOE component.

### 2.7.2 Evaluated configuration – Hardware & OS considerations

Software components 1 & 2 listed in section 2.7 execute on a single Sun SPARC system with a certified or assurance maintained combination of Sun Trusted Solaris 8 and CSB2. The combinations of Sun Trusted Solaris 8 and CSB2 applicable to the certification of the Policy Server are:

- CSB2.1 on Trusted Solaris 8 12/02
- CSB2.2 on Trusted Solaris 8 12/02, 7/03 and 2/04

A rationale for alternative CSB2/TSOL platforms (widening it to any assured derivatives of the above listed versions of CSB2) is provided in Annex J. The range of the specific Sun SPARC systems that form part of the Policy Server system environment is defined by the Multi-platform rationale applicable to the version of CSB2 in use.

Software components 3 & 4 listed in section 2.7 execute on the following platforms which form part of the TOE environment:

- Internet Explorer (V6.0) on Windows 2000 Pro (SP4)
- Internet Explorer (V6.0) on Windows XP Pro (SP2) 32 and 64 bit versions
- Internet Explorer (V6.0) on Windows Server 2003 (R2) 32 and 64 bit versions

A rationale for alternative platforms (widening it to any Windows platform running Internet Explorer V6.0 or later) is provided in Annex K.

Software component 5 listed in section 2.7 executes on the following platforms which form part of the TOE environment:

- SUN JRE 1.4.2 on Windows 2000 Pro (SP4)
- SUN JRE 1.4.2 on Windows XP Pro (SP2) 32 and 64 bit versions
- SUN JRE 1.4.2 on Windows Server 2003 (R2) 32 and 64 bit versions
- SUN JRE 1.4.2 on Linux (Kernel 2.4 and GLIB 2.3, or later)
- SUN JRE 1.4.2 on Solaris (SUN Solaris 8, 9 or 10)

A rationale for alternative platforms (widening it to any platform that supports SUN's JRE 1.4.2 or later) is provided in Annex L.

Hardware specifications for all platforms encompassed within the scope of the evaluated configuration will be detailed in the Certification Report.

### 2.7.3 Evaluated configuration – network topology considerations

The evaluated network configurations encompass all physical and logical configurations as described in section 2.2.

# 3 TOE Security Environment

## 3.1 Secure Usage Assumptions

The following assumptions scope the security problem to be addressed by the TOE by implicitly excluding a number of threats that are to be wholly addressed by measures taken in the assumed environment of the TOE.

### Physical Aspects

A.Physical_Control: **Physical protection of CSDS**
CSDS is assumed to be located in a physical environment that physically protects it against unauthorised access to subscriber and management information stored or in transit through CSDS.

### Personnel Aspects

A.Competent_Admin: **Competent authorised administrators**
Authorised administrators are assumed to be competent and trained to manage CSDS and the security of the information it contains. It is assumed that they are not careless, wilfully negligent or hostile and that they will follow the policies and procedures defined in CSDS documentation for secure administration of CSDS.

A.Review_CSDS_Operation: **Authorised administrators review CSDS operation**
It is assumed that authorised administrators will review audit logs, email notifications and the status of message queues regularly. In the event that the capability to manage Policy Servers is disrupted for a significant period, for example, due to power failure or natural disaster at a ClearPoint Management Station or SPIF Editor, or due to the loss of a remote management connection or compromised DSA, it is assumed that authorised administrators, which may include CSB2 Administrators, will take remedial action in accordance with Company procedures, which may include disabling subscriber message flow by stopping Policy Engines.

### Connectivity Aspects

A.Platform_Admin: **Platform administration**
Administration of the CSB2/TSOL platform is assumed to be performed locally and not via a DMZ network.

A.Policy_Admin: **Policy administration**
Authorised administrators defining or modifying Message Policy are assumed, for any specific Policy Server, to perform the function exclusively as a CSDS Server-mode Administrator, or exclusively as a CSDS Directory-mode Administrator.

A.Remote_Admin: **Remote administration**
It is assumed that CSDS Directory-mode Administrators and X.841 Security (Label) Policy Administrators outside the DMZ network will only be able to define and modify Message Policy and SPIF settings, respectively, and only via DSAs using networks connected to the DMZ network.

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

## 3.2 Threats to Security

The assumed threats to be addressed by the TOE in combination with its environment (IT and non-IT) are listed below, after a brief description of the assets and threat agents.

Assets:
As a boundary protection device, CSDS protects not only TOE assets, but also assets in the connected subscriber networks. Assets are therefore: information, facilities and resources on the connected networks; subscriber messages being processed by the TOE; other TOE/TSF data, including notifications, audit data and Message Policies; TOE/TSF functions, including Policy Engine and queue management.

Threat Agents:
These may be persons, or active IT entities (e.g. processes). CSDS may be attacked from subscriber networks, from networks with connection to the DMZ networks, from a DMZ network or locally via a CSB2/TSOL terminal. Threat agents are:

- authorised users of subscriber networks, or intervening networks, or persons who gain unauthorised access to such networks. They may or may not have legitimate access to email facilities with authorisation to communicate with other networks via CSDS. They may be careless or inexperienced users of the email facilities, users motivated to make casual attempts to breach the email export policy, or persons that are motivated to make concerted attempts to breach the email export policy or attack CSDS, but have a low attack potential (expertise, opportunity, resources)
- authorised administrators of CSDS, CSB2 and TSOL. They are trusted, competent and trained to use (in accordance with their role, a subset of) the administration facilities of CSDS, CSB2 & TSOL in an appropriate manner. They are nevertheless human, and may inadvertently mis-configure a complicated policy. (There is a finite risk that they may, due to pressure of work or for illicit purposes, attempt to access administration facilities outside of their role)
- authorised users of networks used to connect the DMZ network with a remote management network, or persons who gain unauthorised access to such networks. They may be users motivated to make casual attempts to modify email policy, or persons that are motivated to make concerted attempts to breach the email policy or attack CSDS, but have a low attack potential (expertise, opportunity, resources)
- CSDS software. An error in the construction or configuration of CSDS may cause an accidental breach of security. Untrusted third party software may attempt deliberate breach of security.

### Threats

**T.Uncontrolled_Flow** **Uncontrolled Message Flow**
An authorised user or unauthorised person on one subscriber network may attempt to release sensitive information not authorised for release, or compromise the security of another subscriber network by sending information with malicious or inappropriate content.

Here, sensitive information may include unauthorised protocols tunnelled through the authorised message protocols, unauthorised data types or authorised subscriber messages that the recipient is not cleared to receive.

**T.Compromised_Flow** **Message Flow Compromised on Networks**
An authorised user or unauthorised person on one subscriber network, or intervening network, may attempt to send a valid subscriber message spoofing the source identity of another user, or replay a valid message from another user, eavesdrop on or modify messages from another user in transit.

**T.Unauthorised_Access** **Unauthorised Access to Message or TOE**
An authorised user or unauthorised person on a subscriber network or a network connected to a DMZ network may attempt to bypass CSDS policy enforcement, eavesdrop on or modify subscriber messages in transit through CSDS or interfere with CSDS data (Message Policies, message queues, audit logs) by modifying CSDS security data or by exploiting ambiguities in the messaging standards or data types.

**T.Unaccountable_Actions** **Unaccountable Actions**
Authorised users, unauthorised persons or CSDS software components may not be accountable for their actions and attempts to compromise Message Policy and CSDS security.

**T.Complexity** **Mis-Configuration of Message Policy**
Authorised administrators may inadvertently mis-configure Message Policy due to its complexity.

**T.Unauthorised_Admin** **Unauthorised Use of Administration Role**
Authorised administrators may exceed their authority by attempting to perform actions outside of their prescribed role.

**T.Unpredictable** **Unpredictable Application of Message Policy**
CSDS software may perform unpredictable checks and actions due to failures in software or hardware or due to ambiguities in the messaging standards or data types, thus compromising the application of subscriber message policy.

**T.Residual** **Release of Residual Information**
CSDS software may release in the current message residual information from previous messages due to a failure to clear storage resources between the processing of individual messages.

## 3.3 Organisational Security Policies

P.Label: Secure Labelling Policy

CSDS shall be suitable for use in an organisation that mandates, or accepts, use of secure formal message labelling conforming to [X.400], [STANAG 4406] or [S/MIME] standards and optionally to [X.841], or use of informal (text) message labelling in the message's Subject heading field or first line of text.

P.Crypto: Cryptographic Standards and Algorithms

CSDS shall be suitable for use in an organisation that mandates, or accepts, use of secure messaging conforming to [S/MIME] standards and, as a minimum, the following cryptographic algorithms:

- Digital signature: RSA, any required key size, in accordance with [RFC 3447]; DSA, key sizes between 512 and 2048 bits inclusive, in accordance with [FIPS Pub 186]
- Symmetric encryption: AES, minimum 128 bit key size, in accordance with [RFC 3565] and [FIPS Pub 197]; Triple DES, minimum 112 bit key size, in accordance with [ANSI X9.52].
- Key generation: AES, minimum 128 bit key size, in accordance with [RFC 3565] and [FIPS Pub 197]; Triple DES, minimum 112 bit key size, in accordance with [RFC 3370] and [ANSI X9.52]
- Asymmetric encryption for distribution of symmetric keys: Diffie-Hellman, in accordance with [RFC 3370] and [RFC 3565]; RSA, in accordance with [RFC 3370] and [RFC 3565].

# 4 Security Objectives

## 4.1 Security Objectives for the TOE

O.IDAuth: **Unique Identity and Authentication**
The Policy Server must uniquely identify and authenticate the claimed identity of all authorised CSDS Server-mode Administrators before granting them access to Policy Server functions. The TOE must check the authenticity of all Message Policies and SPIFs downloaded to the TOE from a DSA.

O.Management_Enforce: **Security Management Functions**
The TOE must provide role based security management functions that permit authorised TOE administrators to manage the TOE security attributes and data. The TOE must provide a graphical interface which supports clear, consistent and accurate definition and review of those parts of the Message Policy enforced by the Policy Engine and the optional X.841 LSL external library. The TOE must advise TOE administrators of Message Policy checks and actions that are enforced partly or wholly by external libraries.

O.Management_Invoke: **Invoke External Management Functions**
The TOE must correctly invoke those security management functions that permit authorised TOE administrators to manage Message Policy attributes required by the Policy Server external libraries listed in Section 2.6.

O.Auditing: **Auditing of Message Flows and Administrator Actions**
The TOE must provide the capability to record all subscriber message flows and their association with the originator and recipients. The TOE must provide the capability to record TOE administrator selectable details of the application of Message Policy on subscriber message flows. The TOE must record the security relevant actions of TOE administrators. The TOE must provide the capability for TOE administrators to view audit records.

O.Policy_Enforce: **Mediation of Flow of Information**
The TOE must enforce the subscriber message mediation functions that are provided by the Policy Engine and the optional X.841 LSL external library, as defined in Section 2.5.3.

O.Policy_Invoke: **Invocation of Policy Check and Actions**
The TOE must correctly invoke those parts of the Message Policy defined checks and actions that are provided by the Policy Server external libraries listed in Section 2.6.

## 4.2 Security Objectives for the Environment

### Security Objectives for the IT Environment

*Relevant to ClearPoint Management Stations, SPIF Editor Platforms, CSB2/TSOL Platforms, boundary separation devices and packet firewalls:*

OE.IDAuth: **Unique Identity and Authentication**
Authorised administrators of ClearPoint Management Stations, SPIF Editor Platforms, CSB2, TSOL, boundary separation devices and packet firewalls must be uniquely identified and authenticated prior to access to administration functions.

**OE.SecFun: Secure Administration Functions**

ClearPoint Management Stations, SPIF Editor Platforms, CSB2, TSOL, boundary separation devices and packet firewalls must provide secure administration functions that enable management of their security functions (unless the security functions are not relied upon for the security of the TOE e.g. if crypto tokens in ClearPoint or SPIF Editors are held on smart cards).

*Relevant to ClearPoint Management Stations, SPIF Editor Platforms and CSB2/TSOL Platforms:*

**OE.Access_to_PKI_Data: Authorised administrator access to PKI data**

Cryptographic keys and certificate trust points must be protected so that they can only be accessed or modified via authorised TOE and IT Environment functions.

**OE.Policy_Distribution_Integrity: Integrity of distributed Message Policies and SPIFs**

The integrity of Message Policies and SPIFs during upload to a DSA, distribution to a DSA on the DMZ network (possibly via other DSAs or DSA network) and download to a CSDS component, as well as during storage on the DSAs, must be protected by digital signatures, which are verified by the cryptographic subsystem provided on the CSDS component.

*Relevant to CSB2/TSOL Platforms:*

**OE.ConFlo: Controlled Information Flow**

Information must not flow between subscriber networks unless it passes through the Policy Server.

**OE.NoRemo: No Remote Access**

Subscribers and authorised administrators must be unable to directly access a CSDS Server from the Company or World subscriber networks.

**OE.Residual_Info: No Residual Information**

The CSB2/TSOL platform must ensure that residual information from a previous information flow is not transmitted in any way and is unavailable for reuse.

**OE.Accountability: Individual Accountability**

Each CSB2/TSOL platform must ensure that authorised administrators of the CSB2/TSOL platform are held accountable for their actions.

**OE.Auditing: Audit Recording & Reporting**

Each CSB2/TSOL platform must record the security relevant actions of users of the CSB2/TSOL platform, with accurate dates and times. The CSB2/TSOL platform must present this information to authorized administrators.

*Relevant to Policy Servers:*

**OE.Policy_Enforce: External Library Policy Enforcement**

Each Policy Server must enforce those parts of Message Policy defined checks and actions that are provided by Policy Server external libraries (listed in Section 2.5).

OE.Policy_Server_Support: Policy Server External Library Operations
Each Policy Server must provide external library support for cryptographic operations, associated key management and formal security label operations.

*Relevant to ClearPoint Management Stations:*

OE.ClearPoint_Support: ClearPoint External Library Operations
Each ClearPoint Management Station must provide external library support for cryptographic operations, associated key management, formal security label operations and Message Policy management operations.

*Relevant to SPIF Editors:*

OE.SPIF_Editor_Support: SPIF Editor External Library Operations
Each SPIF Editor Platform must provide external library support for cryptographic operations, associated key management and formal security label operations.

*Relevant to boundary separation devices and packet firewalls:*

OE.DOS_Protection: Protection against Denial of Service
CSDS must be protected against Denial of Service attacks.

*Relevant to boundary separation devices:*

OE.Remote_Admin: Remote administration
CSDS Directory-mode Administrators and X.841 Security (Label) Policy Administrators outside the DMZ network shall only be able to define and modify Message Policy and SPIF settings, respectively, and only via DSAs using networks connected to the DMZ network.

OE.DMZ_Protection: Adequate Protection of the DMZ
The DMZ network and each connected CSDS management network must be protected from any other connected network by appropriately assured (up to EAL4/E3) boundary separation devices. These boundary separation devices must provide at least the level of protection from subscriber networks that is provided by CSB2 to its DMZ.

Security Objectives for the Non-IT Environment

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 CSDS documentation for secure administration of CSDS.

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

OE.Policy_Admin: Policy administration

Authorised administrators defining or modifying Message Policy are assumed, for any specific Policy Server, to perform the function exclusively as a CSDS Server-mode Administrator, or exclusively as a CSDS Directory-mode Administrator.

OE.Review_CSDS_Operation: Authorised administrators review CSDS operation

Authorised administrators shall review audit logs, email notifications and the status of message queues regularly. In the event that the capability to manage Policy Servers is disrupted for a significant period, for example, due to power failure or natural disaster at a ClearPoint Management Station or SPIF Editor, or due to the loss of a remote management connection or compromised DSA, authorised administrators, which may include CSB2 Administrators, shall take remedial action in accordance with Company procedures, which may include disabling subscriber message flow by stopping Policy Engines.

OE.Physical_Control: Physical Protection of the CSDS

CSDS must be located in a physical environment that physically protects it against unauthorised access to subscriber and management information stored or in transit through CSDS.

OE.Prot_Against_Nature: Natural disaster protection

Each CSDS Server 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

Each CSDS Server must have adequate backup power sources to ensure that sudden losses of power do not affect availability of service or loss of data.

OE.SecSta: Secure Startup of Service

Authorised administrators shall ensure that procedures and/or mechanisms are in place to ensure that, upon initial start up or recovery from an interruption in service, the CSB2/TSOL platform does not compromise its resources or those of any connected network.

OE.DMZ_Separation: Separation of the DMZ for each direction of flow

Policy Servers (on different instances of a CSDS Server) that are controlling subscriber 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 subscriber message flow in the other direction.

# 5 IT Security Requirements

## 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.

### 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: FAU_GEN.1.1

a) Start-up and shutdown of the audit functions;
b) Changes to the Message Policy;
c) Changes to X.841 SPIFs;
d) Changes to PKI data;
e) Authentication attempts[10];
f) Access exceptions;
g) Subscriber message transactions.

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

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.

Table 5.1 Additional Information in Auditable Events

| Section | Component | Event Type | 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. | |
| 5.1.2.3 | FAU_SAR.1 | Access exceptions. | Reason for failure. |
| 5.1.2.4 | FAU_SEL.1 | None. | |
| 5.1.2.5 | FAU_STG.4X | None. | |
| 5.1.3.1 | FCS_COP.1X | None. | |
| 5.1.4.1 | FDP_IFC.1 | None. | |

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

| Section | Component | Event Type | Additional Information |
|---|---|---|---|
| 5.1.4.2 | FDP_IFF.1 | Subscriber message transactions. | Message identifiers, message subject, message recipients, message security label (if present), details of message processing carried out in accordance with the Message Policy rules. |
| 5.1.4.3 | FDP_LCK.1X | None. | |
| 5.1.4.4 | FDP_LCK.2X | None. | |
| 5.1.4.5 | FDP_SPD.1X | None. | |
| 5.1.4.6 | FDP_TAO.1X | None. | |
| 5.1.4.7 | FDP_TCK.1X | None. | |
| 5.1.4.8 | FDP_VSF.1X | None | |
| 5.1.5.1 | FIA_UAU.2X | Authentication attempts[11]. | Identification of the specific Policy Server (Policy Server ID) on which authentication was performed.<br>If failed – the reason<br>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.<br>If failed – the reason<br>If successful – the granted access control level. |
| 5.1.6.1 | FMT_MOF.1 | None. | |
| 5.1.6.2 | FMT_MSA.1 | Access exceptions. | Reason for failure. |
| 5.1.6.3 | FMT_MSA.3X | None. | |
| 5.1.6.4 | FMT_MTD.1 | Access exceptions. | Reason for failure. |
| 5.1.6.5 | FMT_SMF.1 | Changes to the Message Policy.<br>Changes to X.841 SPIFs.<br>Changes to PKI data. | Message Policy identity.<br>SPIF identity. |
| 5.1.6.6 | FMT_SMF.1X | None. | |
| 5.1.6.7 | FMT_SMR.1 | None. | |

[11] 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.

#### 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[12] that caused the event. FAU_GEN.2.1

Additional dependency: FDP_IFF.1

#### 5.1.2.3 Security audit review (FAU_SAR.1)

The TSF shall provide CSDS Server-mode Administrators having Audit Log Viewing administrator privilege with the capability to read audit information from the audit records. FAU_SAR.1.1

The TSF shall provide the audit records in a manner suitable for the user to interpret the information. FAU_SAR.1.2

#### 5.1.2.4 Security audit event selection (FAU_SEL.1)

The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes: FAU_SEL.1.1

a) Event type (Subscriber message transactions only)
b) Message Policy Relationship
c) Message Policy rule.

#### 5.1.2.5 Prevention of audit data loss (FAU_STG.4X) (explicitly stated)

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

The TSF shall prevent subscriber message transaction events if the audit trail is full. FAU_STG.4X.1

Dependencies: FAU_STG.1 Protected audit trail storage.

### 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
b) DSA
c) Diffie-Hellman
d) Triple DES
e) AES

that meet recognised standards.

Dependencies: FCS_COP.1 Cryptographic operation.

[12] 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.

### 5.1.4 Subscriber data protection (FDP)

#### 5.1.4.1 Subset information flow control (FDP_IFC.1)

The TSF shall enforce the CSDS Message Flow Control Policy[13] on: FDP_IFC.1.1

a) Subjects: Policy Engine
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 or discard of a subscriber message from a queue of type IN; the non-delivery or discard of a subscriber message from a queue of 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 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 Policy Engine's Message Policies
   iii) The Policy Engine's selected Message Policy
b) Information security attributes:
   i) The message's queue type[14]: IN, WORLD, COMPANY, MANUAL
   ii) The message's originator 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[15]
   vii) The message's X.400 information object type (Probe, Delivery Report, Receipt Notification)
   viii) The message's X.400 content type
   ix) The message's X.400 body-part types
   x) The message's MIME types
   xi) The message's message elements and their respective data type
   xii) The messages's SMTP Header field types
   xiii) The message's STANAG 4406 Precedence or X.400 Priority
   xiv) The message's size.

[13] Application Note: The CSDS Message Flow Control Policy is wider in scope than the Message Policy. It is defined by the content of the total set of SFRs that reference it.

[14] Application Note: The message's queue type is the type of message queue holding the message at the start or end of an operation.

[15] 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); or RFC 2634 (from an eSSSecurityLabel authenticated attribute); or STANAG 4406 (from the content-security-label component of the SecurityInformationLabels heading extension field); or X.411 (from the message-security-label envelope extension field).

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 subscriber message from a message queue of type IN to a message queue of type WORLD or COMPANY if all of the implicit CSDS Message Flow Control Policy conditions listed in Table 5.2 are met, and all of the active Message Policy conditions applicable to the subscriber's message and configured for the subscriber message's originator/recipient pair (zero or more of the conditions listed in Table 5.3) are met.

Table 5.2 CSDS Implicit Message Flow Control Policy Pass-Through Conditions

| Implicit CSDS Message Flow Control Policy Conditions for Pass-Through | Enforced By |
|---|---|
| A Message Policy has been activated | TSF |
| The incoming message is successfully parsed as a valid SMTP or X.400 protocol in conformance with relevant [SMTP-MIME], [S/MIME], [STANAG 4406] and [X.400] standards at least to the extent that originators and recipients can be identified | TSF |
| The outgoing message can be successfully constructed into a valid SMTP or X.400 protocol in conformance with relevant [SMTP-MIME], [S/MIME], [STANAG 4406] and [X.400] standards | TSF |
| Policy Engine is not overloaded by the processing of higher precedence subscriber messages | TSF |
| Subscriber message transit times do not exceed maximum permitted transit times | TSF |
| Policy Engine operational thresholds are not exceeded | TSF |

Table 5.3 Message Policy Pass-Through Conditions

| Message Policy Conditions for Pass-Through | Message Policy Rules | Enforced By[16] |
|---|---|---|
| The originator and recipient are within the Domains, Groups and Users (subscribers) defined in the policy tree of the active Message Policy | For all E-mail on this relationship | TSF |
| The incoming message is successfully parsed as a valid SMTP or X.400 protocol in conformance with relevant [SMTP-MIME], [S/MIME], [STANAG 4406] and [X.400] standards | For all E-mail on this relationship | TSF |
| Non-standard protocol extensions are authorised or are removed | Unsupported Protocol Extensions | TSF |
| MIME transfer encoding and character sets that are not supported are authorised or are removed | Unsupported MIME Encoding | TSF |

[16] Application Note: This column shows if the TSF only, an external library in the IT environment only, or both contribute towards enforcement of the Message Policy Rules identified in column 2.

| Message Policy Conditions for Pass-Through | Message Policy Rules | Enforced By[16] |
|---|---|---|
| X.400 information objects[17] other than Messages (i.e. Probes, Delivery Reports) and Receipt Notifications are recognised and authorised (omitting checks for Message Policy conditions that are inapplicable to such objects) | Message Type | TSF |
| [SMTP-MIME] DSNs and MDNs are recognised and authorised (omitting checks for Message Policy conditions that are inapplicable to such objects) | Message Type | TSF |
| Return of original message content is permitted in message types that are reporting status of original message delivery | Returned Content | TSF |
| The message precedence or priority is permitted | X.400 Precedence (Priority) | TSF |
| All X.400 content types are authorised or are removed | X.400 content types | TSF |
| All X.400 body part types are authorised or are removed | X.400 body-part types | TSF |
| All [SMTP-MIME] Headers are authorised or are removed | SMTP Headers | TSF |
| All MIME media types are authorised or are removed | MIME Media Types | TSF |
| The message size is within the configured maximum message size | Size Restriction<br>Size Restriction per Precedence | TSF |
| The incoming PKI state is permitted | Enforce signature/encryption | TSF & cryptographic subsystem |
| If the incoming message is signed, the signatures and associated certificates are authenticated and validated to a configured trust point | Enforce signature/encryption | TSF & cryptographic subsystem |
| If the incoming message is signed, the message's originator identity is consistent, i.e. the originator's email address is contained in the associated user certificate | Enforce signature/encryption | TSF & cryptographic subsystem |
| If the incoming message is encrypted, the message and all embedded encrypted messages can be decrypted | Enforce signature/encryption | TSF & cryptographic subsystem |
| The message contains a valid security label that is dominated by the originator/recipient pair clearance | Security Labelling<br>First Line Labelling<br>Subject Labelling | TSF or formal security label subsystem[18] |
| Message passes spam detection rules | Spam Filtering | Spam detection subsystem |

[17] As defined in [X.402] clause 8

[18] Application Note: The formal security label subsystem is within the TSF when the X.841 LSL option is installed.

| Message Policy Conditions for Pass-Through | Message Policy Rules | Enforced By[16] |
|---|---|---|
| The content of the message's X.400 body-parts and MIME types are (recursively) identified and decomposed into message elements, macros identified and text extracted | Data Type Identification | Data type recognition subsystem |
| Each message element data type is consistent with its internal identification (GUID) and external identification (file-name extension, X.400 body-part type, MIME type) | Data Type Identification | TSF & data type recognition subsystem |
| All message elements are authorised data types or elements are removed | Data Type Identification | TSF |
| All message elements are authorised macro types or elements are modified or removed | Macro Filtering | TSF & data type recognition subsystem[19] |
| All message elements contain no malicious code, or one or more elements contain malicious code and the elements are cleaned or removed | Virus Scanning | VS subsystem |
| Message elements pass textual analysis rules or elements are modified or removed | Textual Analysis | TSF & textual analysis subsystem[19] |
| The formal security label(s) in the message is successfully translated into another security policy and/or another location within the message | Security Label Modification | TSF & formal Security Label subsystem[18] |
| The incoming PKI state can be converted to the specified outgoing PKI state | Signature/Encryption Modification | TSF & cryptographic subsystem |
| If the incoming message is signed, re-signing of the outgoing message is specified, and the message is modified by the Policy Engine, re-signing with the Policy Server's private signature key is permitted | Signature/Encryption Modification | TSF & cryptographic subsystem |

b) The Policy Engine shall be permitted to move a subscriber 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 subscriber message's originator/recipient pair (zero or more of the conditions listed in Table 5.3) are not met.

c) The Policy Engine shall be permitted to non-deliver or discard a subscriber message from a message queue of type IN provided one or more of the implicit CSDS Message Flow Control Policy conditions listed in Table 5.2 are not met or one or more of the active Message Policy conditions configured for the subscriber message's originator/recipient pair (zero or more of the conditions listed in Table 5.3) are not met.

[19] Application Note: When a message element is to be removed such removal is performed entirely by the TSF. Where a subsystem has the capability to modify data (e.g. a data type recognition subsystem removes a macro, or a textual analysis subsystem removes text) then such modification is performed by the subsystem, but the replacement of the modified message element within the message is performed by the TSF.

The TSF shall enforce the following additional rules: FDP_IFF.1.3

a) The Policy Engine shall invoke the implicit CSDS Message Flow Control Policy actions listed in Table 5.4.

Table 5.4  CSDS Implicit Message Flow Control Policy Actions

| Implicit CSDS Message Flow Control Policy Actions | Enforced By[20] |
|---|---|
| Higher precedence subscriber messages are processed before queued subscriber messages of lower precedence | TSF |
| Warning messages to administrators are generated if Policy Engine operational thresholds are exceeded | TSF |

b) Considering each of the Message Policy rules in turn, the Policy Engine shall invoke the actions listed in Table 5.5, if the action is an available attribute of the Message Policy rule under consideration and is configured in the active Message Policy for the subscriber message's originator/recipient pair.

Table 5.5  Message Policy Rule Secondary Actions

| Message Policy Rule Secondary Actions | Enforced By[21] |
|---|---|
| Place a copy of the message in an inbound archive queue prior to the enforcement of the Message Policy | TSF |
| Place a copy of the message in an outbound archive queue subsequent to the enforcement of the Message Policy | TSF |
| Record details of message processing, carried out in accordance with the Message Policy rule, in the audit log for the message transactions event type, as specified in FAU_GEN.1. | TSF |
| Add Message Policy configured text to the message warning the recipient that the message contains a macro or other harmful/disallowed content | TSF |
| Add Message Policy configured text to the message advising the recipient that the message has been modified | TSF |
| Send an information notification message, via the WORLD and/or COMPANY queue, to Message Policy configured individuals and groups, which advises of Message Policy rule triggered events and violations | TSF |
| If the policy rule triggers, Invoke an additional policy rule set | TSF |
| If the policy rule does not trigger, Invoke an additional policy rule set | TSF |

c) The Policy Engine shall invoke the Message Policy rule actions listed in Table 5.6, if the action is configured in the active Message Policy for the subscriber message's originator/recipient pair.

[20] Application Note: This column shows that all of the actions are enforced fully by the TSF.

[21] Application Note: This column shows that all of the actions are enforced fully by the TSF.

Table 5.6 Outgoing Actions of Message Policy Rules

| Outgoing Actions | Message Policy Rules | Enforced By |
|---|---|---|
| The message does not contain a formal security label, and is to have a default label assigned and optionally inserted into the message | Security Labelling | TSF |
| The label in the first line of text or subject field is to be removed | First Line Labelling<br>Subject Labelling | TSF |
| The content of the message's X.400 body-parts and MIME types are (recursively) recomposed | Data Type Identification | Data type recognition subsystem |
| Include Message Policy configured text in the message certifying to the recipient that the message is free from macros | Macro Filtering | TSF |
| Include Message Policy configured text in the message certifying to the recipient that the message is free from malicious code | Virus Scanning | TSF |
| Insert Message Policy configured values in specified attributes of the message | Message Modification | TSF |
| Remove MIME multipart preambles and epilogues | Message Modification | TSF |
| The formal security label(s) in the message are to be translated into another security policy and/or another location within the message | Security Label Modification | TSF & formal Security Label subsystem[18] |
| If the incoming message is signed with an algorithm or key strength that is not specified in the algorithm preferences, re-sign the message with the Policy Server's signature | Signature/Encryption Modification | TSF & cryptographic subsystem |
| If the incoming message is encrypted with an algorithm or key strength that is not specified in the algorithm preferences, re-encrypt the message with the recipient's public encryption key | Signature/Encryption Modification | TSF & cryptographic subsystem |
| If the incoming message is signed, and the message is modified by the Policy Engine, re-sign message with the Policy Server's signature | Signature/Encryption Modification | TSF & cryptographic subsystem |
| If the incoming message is signed, always re-sign the message with the Policy Server's signature | Signature/Encryption Modification | TSF & cryptographic subsystem |
| If the outgoing message is to have a signature added or replaced, sign with a private key whose associated certificate contains the originator email address | Signature/Encryption Modification | TSF & cryptographic subsystem |
| If encrypted, only re-encrypt message with the recipient's public encryption key if the message is modified by the Policy Engine | Signature/Encryption Modification | TSF & cryptographic subsystem |

| Outgoing Actions | Message Policy Rules | Enforced By |
|---|---|---|
| If encrypted, always re-encrypt message with the recipient's public encryption key | Signature/Encryption Modification | TSF & cryptographic subsystem |
| If the incoming message is triple wrapped, select outgoing format from one of: retain the outer signature; replace the outer signature by the Policy Server's signature; add the Policy Server's signature to the outer signature | Signature/Encryption Modification | TSF & cryptographic subsystem |
| Send a notification message to the originator, and/or a recipient, and/or an authorised administrator and/or a PAA, via the WORLD and/or COMPANY queue, for any of the actions listed in Table 5.7 | Notifications | TSF |
| Send an X.400 Non-Delivery Report or SMTP DSN to the originator provided that one was requested in the message, and/or to an authorised administrator and/or a PAA, via the WORLD and/or COMPANY queue, if a message is non-delivered | Notifications | TSF |
| Send an X.400 Delivery Report or SMTP DSN to the originator provided that one was requested in the message, and/or to an authorised administrator and/or a PAA, via the WORLD and/or COMPANY queue, if a message is passed-through or released | Notifications | TSF |

Table 5.7 Actions Permitting Notification Messages

| Actions Permitting Notification Messages |
|---|
| Message is passed through or released |
| Message is queued for manual intervention |
| A message element is modified or removed |
| Message is non-delivered |
| Malicious code is detected |
| Message fails textual analysis checks |

d) 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) Same as the PKI state of the subscriber message as received in the IN queue

ii) Plain

iii) Signed

iv) 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[22] between CSB2 VET IN, OUT and RETURN queues and the corresponding Policy Engine IN, WORLD and COMPANY queues[23]
d) A number of Policy Engine MANUAL [24] queues specified in the Message Policy, in the same CSB2 VET compartment
e) For a subscriber message having multiple recipients, the capability to identify recipient groups for those recipients having the same applicable Message Policy settings
f) For each subscriber message received, the capability to apply in accordance with FDP_IFF.1.2 and FDP_IFF.1.3, separately for each identified recipient group, the specific Message Policy rules that are associated with the originator/recipient (group) pair
g) For a subscriber message received with multiple distinct signatures (originators), the capability to determine and apply in accordance with FDP_IFF.1.2 and FDP_IFF.1.3, for each recipient group in the case of multiple recipients, the originator/recipient (group) pair whose specific Message Policy rules result in the least restrictive primary action.

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

a) A CSDS Server-mode Administrator, having Queue Management administrator privilege, 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 subscriber message that was held in the MANUAL queue).

The TSF shall explicitly deny an information flow based on the following rules: FDP_IFF.1.6

a) A CSDS Server-mode Administrator, having Queue Management administrator privilege, shall be permitted to authorise the non-delivery or discard (permanent deletion) of a subscriber message from a message queue of type MANUAL.

[22] 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).

[23] 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.

[24] Application Note: The CSDS MANUAL queues are defined and named within each Message Policy (by a CSDS Server-mode Administrator with Message Policy Administration administrator privilege or a CSDS Directory-mode Administrator), and CSDS Server-mode Administrators with Queue Management or Queue Viewing administrator privilege are then given access to any (populated) MANUAL queues. CSDS MANUAL queues do not correspond with the CSB2 REJECT queue, which is not used in CSDS.

### 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 subscriber message security label validity and clearance checking, label mapping and label textual rendering operations. FDP_LCK.1X.1

Dependencies: [FDP_LCK.2X X.841 formal security label checking operations OR
FDP_LCK.3X Formal security label checking operations].

### 5.1.4.4 X.841 formal security label checking operations (FDP_LCK.2X) (explicitly stated)

Hierarchical to: No other components.

The TSF shall have the capability to use Security (Label) Policy information contained in X.841 SPIFs to: FDP_LCK.2X.1

a) check the validity of a given subscriber message formal security label
b) check that a given formal security label is dominated by a specified clearance
c) map a given formal security label from one X.841 Security (Label) Policy to another X.841 Security (Label) Policy
d) render a given formal security label into text.

Dependencies: No dependencies.

### 5.1.4.5 Calls to spam detection operations (FDP_SPD.1X) (explicitly stated)

Hierarchical to: No other components.

The TSF shall perform properly formed calls to spam detection operations. FDP_SPD.1X.1

Dependencies: FDP_SPD.2X Spam detection operations.

### 5.1.4.6 Calls to textual analysis operations (FDP_TAO.1X) (explicitly stated)

Hierarchical to: No other components.

The TSF shall perform properly formed calls to textual analysis operations. FDP_TAO.1X.1

Dependencies: FDP_TAO.2X Textual analysis operations.

### 5.1.4.7 Calls to data type checking operations (FDP_TCK.1X) (explicitly stated)

Hierarchical to: No other components.

The TSF shall perform properly formed calls to data type checking (including macro detection) operations. FDP_TCK.1X.1

Dependencies: FDP_TCK.2X data type checking operations.

### 5.1.4.8 Calls to Virus Scanner operations (FDP_VSF.1X) (explicitly stated)

Hierarchical to: No other components.

The TSF shall perform properly formed calls to Virus Scanner operations. FDP_VSF.1X.1

Dependencies: FDP_VSF.2X Virus Scanner 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 Policy Server shall require each CSDS Server-mode Administrator to be successfully authenticated[25] by appropriate calls to cryptographic operations before allowing any other Policy Server mediated actions on behalf of that user. FIA_UAU.2X.1

The TSF shall require the authenticity of each Message Policy and SPIF downloaded from a DSA to be successfully validated by appropriate calls to cryptographic operations before allowing use of the Message Policy or SPIF by CSDS Directory-mode Administrators, X.841 Security (Label) Policy Administrators or Policy Servers. FIA_UAU.2X.2

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 Policy Server shall require each CSDS Server-mode Administrator to identify itself[26] by appropriate calls to cryptographic operations before allowing any other Policy Server mediated actions on behalf of that user. FIA_UID.2X.1

Dependencies: FCS_COP.1X Calls to cryptographic operations.

### 5.1.6 Security management (FMT)

#### 5.1.6.1 Management of security attributes (FMT_MOF.1)

The TSF shall restrict the ability to disable and enable the functions of subscriber message flow to a CSDS Server-mode Administrator having one or more of the Message Policy Selection, Policy Server Configuration Administration or Diagnostic Log Configuration administrator privileges[27]. FMT_MOF.1.1

#### 5.1.6.2 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) A CSDS Directory-mode Administrator shall be permitted to view, define and modify the behaviour of a Message Policy

[25] Application Note: Authentication is performed by the cryptographic operations on a Policy Server.

[26] Application Note: Identification is performed by the cryptographic operations on a Policy Server.

[27] Application Note: A CSB2 Administrator acting in the tms role (or in the cots role associated with the Policy Server) also has the ability to disable and enable the TOE functions of subscriber message flow. Other IT Environment administrators may have the ability to disable and enable IT Environment components on which the TOE is dependent (e.g. TSOL, DSAs), or on which subscriber message flow to/from the TOE is dependent (e.g. packet firewalls, Border MTAs).

b) A CSDS Server-mode Administrator having Message Policy Administration administrator privilege shall be permitted to view, define and modify the behaviour of a Message Policy

c) A CSDS Server-mode Administrator having Message Policy Viewing administrator privilege shall be permitted to view a Message Policy

d) A CSDS Server-mode Administrator having Message Policy Selection administrator privilege shall be permitted to view, select and activate a Message Policy

e) An X.841 Security (Label) Policy Administrator (optional) shall be permitted to view, define and modify the content of an X.841 SPIF.

### 5.1.6.3 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.

### 5.1.6.4 Management of Policy Server data (FMT_MTD.1)

The TSF shall restrict the ability to perform the operations listed in Table 5.8 on the Policy Server data listed in Table 5.8 to the CSDS Server-mode Administrator having the administrator privileges listed in Table 5.8. FMT_MTD.1.1

Table 5.8 Policy Server Data Management Functions

| Policy Server Data Management Functions | Administrator Privilege |
|---|---|
| Define, view and modify Policy Server Configuration Data[28] | Policy Server Configuration Administration |
| View Policy Server Configuration Data | Policy Server Configuration Viewing |
| Authorise subscriber message release, non-delivery or discard actions from the MANUAL queues and view the status of message queues | Queue Management |
| View the status of message queues (including mqueue_in, mqueue_out, bad) | Queue Viewing |
| Search for and view subscriber messages in the archive queues arch_in and arch_out | Archive Viewing |
| View the contents of audit log files | Audit Log Viewing |
| Configuration and display of diagnostic logs | Diagnostic Log Configuration |

### 5.1.6.5 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 content of an X.841 SPIF

[28] Application Note: Policy Server Configuration Data is defined in Annex B.

b) Define and modify the behaviour of a Message Policy[29], using a graphical interface that:

   i) Provides for clear, consistent and accurate definition and review of the Message Policy relationships and rules

   ii) Advises CSDS Directory-mode Administrators and CSDS Server-mode Administrators of Message Policy checks and actions that are partly or fully enforced by external libraries

c) Select a Message Policy

d) Activate a Message Policy[30]

e) Stop and start a Policy Engine

f) Manage functions listed in Table 5.8, Table 5.9, Table 5.10 and Table 5.11.

Table 5.9 Policy Server PKI Data Management Functions

| Policy Server PKI Data Management Functions |
|---|
| Add, delete, edit and list crypto tokens (containing private keys) |
| Add, delete and list certificate trust points |
| Add, delete, edit and list DSA details, specifying DAP or LDAP communication protocol |
| Add, delete and list identification of user certificates for the authentication of CSDS Server-mode Administrators with appropriate administrator privileges, CSDS Directory-mode Administrators and X.841 Security (Label) Policy Administrators |
| Define parameters used for checking the integrity of Message Policies, SPIFs, spam definition updates and malicious code definition updates downloaded from a DSA |
| Specify synchronisation intervals for Message Policies, SPIFs, spam definition updates and malicious code definition updates downloaded from a DSA |

Table 5.10 ClearPoint PKI Data Management Functions

| ClearPoint PKI Data Management Functions |
|---|
| Add, delete, edit and list crypto tokens (containing private keys) |

[29] Application Note: Message Policy consists of sets of policy rules between pairs of objects (policy relationships), 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 rules at one level of the hierarchy are inherited by lower levels, unless an explicit exception policy is set at the lower levels. The contents of a Message Policy are described in Annex A.

[30] Application Note: When a change is made by a CSDS Directory-mode Administrator using ClearPoint in Directory-mode 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 using ClearPoint in Server-mode to an active Message Policy, the change will only be loaded into the Policy Engine by an explicit action of a CSDS Server-mode Administrator having Message Policy Selection administrator privilege, or when the Policy Engine is re-started.

| ClearPoint PKI Data Management Functions |
|---|
| Add, delete and list certificate trust points |
| Add, delete and list identification of user certificates |
| Add, delete, edit and list DSA details, specifying DAP or LDAP communication protocol |

Table 5.11 SPIF Editor PKI Data Management Functions

| SPIF Editor PKI Data Management Functions |
|---|
| Add, delete, edit and list crypto tokens (containing private keys) |
| Add, delete and list certificate trust points |
| Add, delete and list identification of user certificates |
| Add, delete, edit and list DSA details, specifying DAP or LDAP communication protocol |

#### 5.1.6.6 Call to Management Functions (FMT_SMF.1X)

Hierarchical to: No other components.

ClearPoint shall perform properly formed calls to ClearPoint external management functions. FMT_SMF.1X.1

Dependencies: FMT_SMF.1 Specification of management functions (IT-Environment).

#### 5.1.6.7 Security roles (FMT_SMR.1)

The TSF shall maintain the roles: FMT_SMR.1.1

a) CSDS Server-mode Administrator,
b) CSDS Directory-mode Administrator,
c) X.841 Security (Label) Policy Administrator (optional).

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

### 5.1.7 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 Policy Server relies on CSB2, which in turn relies on TSOL to provide some protection.

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

CSDS Policy Server also relies on a number of external libraries in the IT environment, as follows:

a) A selected cryptographic subsystem to perform cryptographic operations and associated key management, the security requirements for which are described in Section 5.3.2
b) A selected formal security label subsystem to perform security label checking operations (except when the X.841 LSL external library option is installed), the security requirements for which are described in Paragraph 5.3.3.1
c) Zero or more selected VS subsystems to scan subscriber message elements to identify malicious code, the security requirements for which are described in Paragraph 5.3.3.5
d) Zero or more selected subsystems to perform textual analysis operations, the security requirements for which are described in Paragraph 5.3.3.3
e) Zero or more selected subsystems to perform data type checking operations (including macro detection), the security requirements for which are described in Paragraph 5.3.3.4
f) Zero or more selected subsystems to perform spam detection, the security requirements for which are described in Paragraph 5.3.3.2.

In order to operate in a secure manner ClearPoint relies on Microsoft Windows' implementation of selected SFRs that are required to comply with [CAPP].

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

a) A selected cryptographic subsystem to perform cryptographic operations and associated key management, the security requirements for which are described in Section 5.3.2
b) A selected formal security label subsystem to perform security label checking operations (when the X.841 LSL external library option is excluded), the security requirements for which are described in Paragraph 5.3.3.1
c) Zero or more selected external management subsystems for configuration of Policy Server external libraries, the security requirements for which are described in Section 5.3.4
d) A cryptographic library accessed through the Microsoft CryptoAPI to communicate with the Policy Server Administration Service via the SOAP/XML protocols over HTTP over SSL, the security requirements for which are described in Section 5.3.2.

In order to operate in a secure manner SPIF Editor relies on Microsoft Windows', Solaris' or Linux's implementation of selected SFRs that are required to comply with [CAPP].

SPIF Editor relies on the following external library:

a) A selected cryptographic subsystem to perform cryptographic operations and associated key management, the security requirements for which are described in Section 5.3.2.

CSDS (Policy Server, ClearPoint Management Station and SPIF Editor) also relies on the use of the cryptographic subsystem digital signature operations to verify the integrity of Message Policies and X.841 SPIFs received from a DSA, the security requirements for which are described in Section 5.3.5.

CSDS Policy Server also relies on packet firewalls, implemented on separate hardware from that required to run CSDS software, which implement security functions that protect CSDS Policy Servers and the CSB2/TSOL platform from denial of service attacks (OE.DOS_Protection) originating from the subscriber networks.

Finally, CSDS relies on boundary separation devices, implemented on separate hardware from that required to run CSDS software, which implement security functions (appropriately assured up to EAL4/E3) that protect CSDS components as follows:

a) Policy Servers, SPIF Editors and ClearPoint Management Stations from denial of service attacks (OE.DOS_Protection) originating from networks attached to a DMZ network or from networks attached to a remote management network
b) Policy Servers, SPIF Editors and ClearPoint Management Stations from unauthorised access from networks attached to a DMZ network or a remote management network (OE.DMZ_Protection)
c) Policy Servers from any attempted changes to a Policy Server by remote TOE Administrators from networks attached to a DMZ network, except for changes to Message Policy settings made by CSDS Directory-mode Administrators and changes to SPIF settings made by X.841 Security (Label) Policy Administrators (OE.Remote_Admin).

In order to provide the security functions described in the previous two paragraphs, as a minimum the following SFRs are required to be implemented by the packet firewalls and boundary separation devices:

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.

## 5.3.2 Cryptographic support (FCS)

### 5.3.2.1 Cryptographic Key Generation (FCS_CKM.1)[31]

The cryptographic subsystem shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Triple DES and specified cryptographic key sizes of at least 112 bits that meet the following: [RFC 3370] and [ANSI X9.52]. FCS_CKM.1.1;1

The cryptographic subsystem shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm AES and specified cryptographic key sizes of at least 128 bits that meet the following: [RFC 3565] and [FIPS Pub 197]. FCS_CKM.1.1;2

### 5.3.2.2 Cryptographic key distribution (FCS_CKM.2)[32]

The cryptographic subsystem shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method key agreement using Diffie-Hellman that meets the following: [RFC 3370] and [RFC 3565]. FCS_CKM.2.1;1

The cryptographic subsystem shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method key transport using RSA that meets the following: [RFC 3370] and [RFC 3565]. FCS_CKM.2.1;2

### 5.3.2.3 Cryptographic key destruction (FCS_CKM.4)

The cryptographic subsystem 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)[33]

The cryptographic subsystem shall perform digital signature operations in accordance with a specified cryptographic algorithm RSA and cryptographic key sizes any required that meet the following: [RFC 3447]. FCS_COP.1.1;1

The cryptographic subsystem shall perform digital signature operations in accordance with a specified cryptographic algorithm DSA and cryptographic key sizes of between 512 and 2048 bits inclusive that meet the following: [FIPS Pub 186]. FCS_COP.1.1;2

The cryptographic library accessed through the Microsoft CryptoAPI shall perform digital signature operations in accordance with a specified cryptographic algorithm RSA and cryptographic key sizes any required that meet the following: [RFC 3447]. FCS_COP.1.1;3

The cryptographic library accessed through the Microsoft CryptoAPI shall perform digital signature operations in accordance with a specified cryptographic algorithm DSA and cryptographic key sizes of between 512 and 2048 bits inclusive that meet the following: [FIPS Pub 186]. FCS_COP.1.1;4

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

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

[33] Application Note: The IT Environment may be extended to include cryptographic operations in accordance with other algorithms, key sizes and standards. Microsoft CryptoAPI is used only by ClearPoint in Server-mode in support of I&A-1. Symmetric encryption is used only by the Policy Engine in support of POLICY-2 and POLICY-12.

The cryptographic subsystem 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;5

The cryptographic subsystem shall perform symmetric encryption in accordance with a specified cryptographic algorithm AES and cryptographic key sizes of at least 128 bits that meet the following: [RFC 3565] and [FIPS Pub 197]. FCS_COP.1.1;6

## 5.3.3 User Data Protection (FDP)

### 5.3.3.1 Formal security label checking operations (FDP_LCK.3X) (explicitly stated)

Hierarchical to: No other components.

The formal security label subsystem shall have the capability to: FDP_LCK.3X.1

a) check the validity of a given subscriber message formal security label
b) check that a given formal security label is dominated by a specified clearance
c) map a given formal security label from one Security (Label) Policy to another Security (Label) Policy
d) render a given formal security label into text.

Dependencies: No dependencies.

### 5.3.3.2 Spam detection operations (FDP_SPD.2X) (explicitly stated)

Hierarchical to: No other components.

The spam detection subsystem shall have the capability to scan subscriber message elements in order to detect spam corresponding to a set of spam definitions. FDP_SPD.2X.1

Dependencies: No dependencies.

### 5.3.3.3 Textual analysis operations (FDP_TAO.2X) (explicitly stated)

Hierarchical to: No other components.

The textual analysis subsystem shall have the capability to scan subscriber message elements in order to detect textual content in accordance with specific algorithms. FDP_TAO.2X.1

Dependencies: No dependencies.

### 5.3.3.4 Data type checking operations (FDP_TCK.2X) (explicitly stated)

Hierarchical to: No other components.

The data type recognition subsystem shall have the capability to scan subscriber message elements in order to detect the data type of content (including macros) and if the type comprises a single message element extract the textual content from the identified data type. FDP_TCK.2X.1

If the identified data type is a compound object that can contain multiple message elements, then the IT environment may provide the capability to extract the contained message elements from it, and (if possible) to reassemble message elements into a compound object of this data type. FDP_TCK.2X.2

Dependencies: No dependencies.

### 5.3.3.5 Virus Scanner operations (FDP_VSF.2X) (explicitly stated)

Hierarchical to: No other components.

The VS subsystem shall have the capability to scan subscriber message elements in order to detect malicious code corresponding to a set of malicious code definitions. [FDP_VSF.2X.1]

Dependencies: No dependencies.

## 5.3.4 Security management (FMT)

### 5.3.4.1 Specification of Management Functions (FMT_SMF.1)

The ClearPoint external management subsystems shall be capable of performing the following security management functions: [FMT_SMF.1.1]

a) Define and modify Message Policy attributes associated with the following Policy Server external libraries:
   - i) Data type recognition, decomposition, text extraction, macro detection and re-composition
   - ii) Textual analysis
   - iii) Virus scanning
   - iv) Spam detection

b) Supply capability data for the following Policy Server external libraries to enable ClearPoint to define and modify Message Policy attributes associated with:
   - v) Cryptographic operations
   - vi) Formal security label operations (other than the X.841 LSL option which is within the TOE).

## 5.3.5 Protection of the TSF (FPT)

### 5.3.5.1 Inter-TSF detection of modification (FPT_ITI.1)

The cryptographic subsystem shall provide the capability to detect modification of all TSF and 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 cryptographic subsystem shall provide the capability to verify the integrity of all TSF and 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 Administrators' Management Functions[34]

MANAGE-1: The PKI Configuration Utility installed on each Policy Server enables CSB2 Administrators acting in the cots role applicable to the Policy Server to manage the Policy Server PKI data by performing those operations listed in Table 5.9.

MANAGE-2: ClearPoint enables ClearPoint Management Station Administrators to manage the ClearPoint PKI data by performing those operations listed in Table 5.10.

MANAGE-3: The SPIF Editor enables SPIF Editor Platform Administrators to manage the SPIF Editor PKI data by performing those operations listed in Table 5.11.

MANAGE-4: ClearPoint enables CSDS Server-mode Administrators having Diagnostic Log Configuration administrator privilege to configure and view diagnostic logs and to stop/start a Policy Engine.

MANAGE-5: ClearPoint enables CSDS Server-mode Administrators having Audit Log Viewing administrator privilege to view the contents of audit logs.

MANAGE-6: ClearPoint enables CSDS Server-mode Administrators having Archive Viewing administrator privilege to search for and view subscriber messages in archives.

MANAGE-7: ClearPoint enables CSDS Server-mode Administrators having Queue Viewing administrator privilege to view the status of messages in queues.

MANAGE-8: ClearPoint enables CSDS Server-mode Administrators having Queue Management administrator privilege to view the status of messages in queues and to authorise the release, non-delivery or discard of subscriber messages in MANUAL queues.

MANAGE-9: ClearPoint enables CSDS Server-mode Administrators having Policy Server Configuration Viewing administrator privilege to view Policy Server attributes listed in Annex B.

MANAGE-10: ClearPoint enables CSDS Server-mode Administrators having Policy Server Configuration Administration administrator privilege to configure message archives, audit logs and other Policy Server attributes listed in Annex B and to stop/start a Policy Engine.

MANAGE-11: ClearPoint enables CSDS Server-mode Administrators having Message Policy Viewing administrator privilege to view a Message Policy.

MANAGE-12: ClearPoint enables CSDS Server-mode Administrators having Message Policy Selection administrator privilege to view, select and activate a Message Policy and to stop/start a Policy Engine.

MANAGE-13: ClearPoint enables CSDS Server-mode Administrators having Message Policy Administration administrator privilege and CSDS Directory-mode Administrators to view, define and modify the behaviour of a Message Policy, including, via an interface to external

[34] Application Note: This section defines management functions that are available to specific roles, including CSDS Server-mode Administrators having specific administrator privileges; however, the restriction to specific roles and privileges is enforced by AC-1.

management functions, attributes required by the Policy Server external libraries, using a graphical interface that:

a) Provides for clear, consistent and accurate definition and review of the Message Policy relationships and rules

b) Advises CSDS Server-mode Administrators and CSDS Directory-mode Administrators of Message Policy checks and actions that are partly or fully enforced by external libraries.

MANAGE-14: A SPIF Editor (optional) enables X.841 Security (Label) Policy Administrators to view, define and modify the content of an X.841 SPIF.

### 6.1.2 CSB2 Configuration

CSB2-1: A CSDS Server is based on CSB2 configured as follows:

a) Two active CSB2 channels, each comprising a single VET compartment and two PROXY compartments, one for each direction of subscriber message flow through the CSDS Server

b) A CSDS Policy Server installed in each VET compartment.

### 6.1.3 Queue Management Functions

QUEUE-1: The Q-handler Service in each Policy Server moves inbound subscriber messages from the CSB2 IN queue to the Policy Engine IN queue, and moves outbound subscriber messages from the Policy Engine WORLD and COMPANY queues to the:

a) CSB2 OUT and CSB2 RETURN queues respectively, if the direction of subscriber message flow is from COMPANY to WORLD

b) CSB2 RETURN and CSB2 OUT queues respectively, if the direction of subscriber message flow is from WORLD to COMPANY.

### 6.1.4 Message Policy Functions

POLICY-1: Subscriber messages will not be processed by the Policy Engine until a Message Policy has been selected and activated.

POLICY-2: The Policy Engine will accept subscriber messages from a subscriber network in any of the following states:

a) Neither signed or 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.

POLICY-3: For each subscriber message received (in the Policy Engine IN queue), the Policy Engine unpacks the message and validates its conformance with relevant [SMTP-MIME], [S/MIME], [STANAG 4406] and [X.400] standards.

POLICY-4: For each subscriber message received, the Policy Engine identifies all originator/recipient pairs and validates that they are within the domains defined and controlled by the active Message Policy.

POLICY-5: For each subscriber message received having multiple recipients, the Policy Engine identifies recipient groups for those recipients having the same applicable Message Policy settings.

POLICY-6: For each unique originator/recipient (group) pair of a received subscriber message, the Policy Engine determines the specific Message Policy rules configured in the active Message Policy for that originator/recipient (group) pair.

POLICY-7: For each subscriber message received having multiple originators, the Policy Engine determines, for each recipient (group), the least restrictive set of Message Policy rules configured in the active Message Policy from the set of originator/recipient (group) pairs, where restriction is defined by the primary action applied to the subscriber message. Primary actions are, in increasing order of restriction: pass-through (unmodified); pass-through (with message element(s) cleansed or removed); queue for manual intervention; non-deliver (delete with notification), discard (delete without notification).

POLICY-8: For each subscriber message received, the Policy Engine invokes, separately for each identified recipient group, the specific Message Policy rules configured in the active Message Policy for the originator/recipient (group) pair that are applicable to that message.

POLICY-9: The Policy Engine enforces those checks, or parts of checks, listed in Table 5.2 and Table 5.3 as being performed wholly or partly by the TSF.

POLICY-10: The Policy Engine enforces those actions, or parts of actions, listed in Table 5.4, Table 5.5 and Table 5.6 as being performed wholly or partly by the TSF.

POLICY-11: For each recipient of a received subscriber message, the Policy Engine enforces the primary action determined, separately for each identified recipient group, by the application of the checks listed in Table 5.2 and Table 5.3. Primary actions are: pass-through (unmodified); pass-through (with message element(s) cleansed or removed); queue for manual intervention; non-deliver (delete with notification), discard (delete without notification).

POLICY-12: The Policy Engine ensures that subscriber messages leave CSDS in one of the following states:

a) Same as the PKI state of the subscriber message as received in the IN queue;
b) Neither signed nor encrypted;
c) Signed but not encrypted
d) Triple wrapped.

### 6.1.5 Identification and Authentication

I&A-1: All CSDS Server-mode Administrators must successfully complete an identification and authentication process before any interaction with the Policy Server is possible. This is achieved using individual authenticated certificates.

I&A-2: All Message Policies uploaded from ClearPoint to a DSA must be cryptographically signed using the private key of the CSDS Directory-mode Administrator that defined or modified the Message Policy.

I&A-3: All Message Policies downloaded from a DSA to ClearPoint, or to the Policy Server, must successfully complete validation of the digital signature and associated individual authenticated certificate before allowing use of the Message Policy.

I&A-4: All SPIFs uploaded from a SPIF Editor to a DSA must be cryptographically signed using the private key of the X.841 Security (Label) Policy Administrator that defined or modified the SPIF.

I&A-5: All SPIFs downloaded from a DSA to a SPIF Editor, to ClearPoint, or to the Policy Server, must successfully complete validation of the digital signature and associated individual authenticated certificate before allowing use of the SPIF.

### 6.1.6 Access Control

AC-1: The Policy Server restricts access to Policy Server facilities to administrators acting in specific roles, as follows:

a) An X.841 Security (Label) Policy Administrator (optional) may define and modify the content of an X.841 SPIF downloaded from a DSA to a Policy Server
b) A CSDS Directory-mode Administrator may define and modify the behaviour of a Message Policy downloaded from a DSA to a Policy Server
c) A CSDS Server-mode Administrator with appropriate administrator privileges may view, define, modify, select and activate a Message Policy, stop/start a Policy Engine and perform the management functions listed in Table 5.8.

### 6.1.7 Auditing

AUD-1: As a minimum the Policy Server logs the following events:

a) Authentication attempts
b) Start-up and shutdown of Policy Server audit functions and associated details
c) Changes to the Message Policy
d) Changes to X.841 SPIFs (if the optional X.841 LSL external library is installed)
e) Changes to PKI data
f) Access exceptions
g) Subscriber message transactions.

AUD-2: The Policy Server log records for each event:

a) Date
b) Time
c) Type of event
d) Subject identity (the originator email address and/or Distinguished Name in the case of subscriber message transactions; 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 and X.841 SPIFs)
e) Success or failure of the attempt
f) Additional information for specific events, as specified in Table 5.1.

AUD-3: The Policy Engine prevents further processing of subscriber messages if the Policy Engine audit log is full.

### 6.1.8 Encryption

CRYPTO-1: The CSDS components include an interface to cryptographic functions that perform the following operations:

a) RSA digital signature operations in accordance with [RFC 3447]
b) DSA digital signature operations in accordance with [FIPS Pub 186]

c) Triple DES symmetric encryption operations in accordance with [ANSI X9.52]
d) AES symmetric encryption operations in accordance with [RFC 3565] and [FIPS Pub 197]
e) Diffie-Hellman asymmetric encryption operations for the distribution of Triple DES symmetric keys in accordance with [RFC 3370]
f) Diffie-Hellman asymmetric encryption operations for the distribution of AES symmetric keys in accordance with [RFC 3565]
g) RSA asymmetric encryption for the distribution of Triple DES symmetric keys in accordance with [RFC 3370]
h) RSA asymmetric encryption for the distribution of AES symmetric keys in accordance with [RFC 3565]
i) Validation of certificate paths to configured trust points as specified in [X.509].

### 6.1.9 Label Checking

LABEL-1: The Policy Engine and ClearPoint include an interface to subscriber message formal security label checking functions that perform the following operations:

a) Check the validity of a given formal security label
b) Check that the given formal security label is dominated by a specified clearance
c) Translate a value of a formal security label into a value in another security policy
d) Provide a text rendition of the value of a formal security label.

LABEL-2: The optional X.841 LSL external library enforces the subscriber message security label checking functions of LABEL-1 using Security (Label) Policy information contained in X.841 SPIFs.

### 6.1.10 Virus Scanning

VS-1: The Policy Engine includes an interface that calls appropriate Virus Scanner operations correctly.

### 6.1.11 Macro Detection

MACRO-1: The Policy Engine includes an interface that calls appropriate macro detection operations correctly.

### 6.1.12 Spam Detection

SPAM-1: The Policy Engine includes an interface that calls appropriate spam detection operations correctly.

### 6.1.13 Textual Analysis

TEXT-1: The Policy Engine includes an interface that calls appropriate textual analysis operations correctly.

### 6.1.14 Data Type Checking

TYPE-1: The Policy Engine includes an interface that calls appropriate data type checking operations 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.Physical_Control | OE.Physical_Control |
| A.Competent_Admin | OE.Admin, OE.Admin_Docs |
| A.Review_CSDS_Operation | OE.Review_CSDS_Operation |
| A.Platform_Admin | OE.Platform_Admin |
| A.Policy_Admin | OE.Policy_Admin |
| A.Remote_Admin | OE.Remote_Admin |
| A.DMZ_Separation | OE.DMZ_Separation |
| T.Uncontrolled_Flow | O.Policy_Enforce, O.Policy_Invoke, OE.Policy_Enforce |
| T.Compromised_Flow | O.Policy_Enforce, O.Policy_Invoke, OE.Policy_Enforce |
| T.Unauthorised_Access | O.IDAuth, O.Policy_Enforce, OE.IDAuth, OE.ConFlo, OE.NoRemo, OE.DOS_Protection, OE.DMZ_Protection, OE.Policy_Distribution_Integrity, OE.ClearPoint_Support, OE.SPIF_Editor_Support, OE.Policy_Server_Support |
| T.Unaccountable_Actions | O.IDAuth, O.Policy_Enforce, O.Auditing, OE.IDAuth, OE.Accountability, OE.Auditing |
| T.Complexity | O.Management_Enforce, OE.DMZ_Separation |
| T.Unauthorised_Admin | O.IDAuth, OE.IDAuth, O.Management_Enforce, O.Management_Invoke, OE.SecFun, OE.Access_to_PKI_Data, OE.ClearPoint_Support, OE.SPIF_Editor_Support, OE.Policy_Server_Support |
| T.Unpredictable | O.Policy_Enforce, OE.SecSta, OE.Prot_Against_Nature, OE.Prot_Agnst_Pwr_Fail |
| T.Residual | O.Policy_Enforce, OE.Residual_Info |

| Assumption/Threat/Policy | Objectives |
|---|---|
| P.Label | O.Management_Enforce, O.Management_Invoke, O.Policy_Enforce, O.Policy_Invoke, OE.Policy_Enforce, OE.ClearPoint_Support, OE.SPIF_Editor_Support |
| P.Crypto | O.Management_Enforce, O.Management_Invoke, O.Policy_Enforce, O.Policy_Invoke, OE.Policy_Enforce, OE.ClearPoint_Support |

### 7.1.2 Assumptions

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

A.Physical_Control: **Physical protection of CSDS**
CSDS is assumed to be located in a physical environment that physically protects it against unauthorised access to subscriber and management information stored or in transit through CSDS.

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

A.Competent_Admin: **Competent authorised administrators**
Authorised administrators are assumed to be competent and trained to manage CSDS and the security of the information it contains. It is assumed that they are not careless, wilfully negligent or hostile and that they will follow the policies and procedures defined in CSDS documentation for secure administration of CSDS.

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

A.Review_CSDS_Operation: **Authorised administrators review CSDS operation**
It is assumed that authorised administrators will review audit logs, email notifications and the status of message queues regularly. In the event that the capability to manage Policy Servers is disrupted for a significant period, for example, due to power failure or natural disaster at a ClearPoint Management Station or SPIF Editor, or due to the loss of a remote management connection or compromised DSA, it is assumed that authorised administrators, which may include CSB2 Administrators, will take remedial action in accordance with Company procedures, which may include disabling subscriber message flow by stopping Policy Engines.

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

A.Platform_Admin: **Platform administration**
Administration of the CSB2/TSOL platform is assumed to 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 defining or modifying Message Policy are assumed, for any specific Policy Server, to perform the function exclusively as a CSDS Server-mode Administrator, or exclusively as a CSDS Directory-mode Administrator.

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

**A.Remote_Admin: Remote administration**
It is assumed that CSDS Directory-mode Administrators and X.841 Security (Label) Policy Administrators outside the DMZ network will only be able to define and modify Message Policy and SPIF settings, respectively, and only via DSAs using networks connected to the DMZ network.

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

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

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

### 7.1.3 Threats

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

**T.Uncontrolled_Flow Uncontrolled Message Flow**
An authorised user or unauthorised person on one subscriber network may attempt to release sensitive information not authorised for release, or compromise the security of another subscriber network by sending information with malicious or inappropriate content.

Here, sensitive information may include unauthorised protocols tunnelled through the authorised message protocols, unauthorised data types or authorised subscriber messages that the recipient is not cleared to receive.

T.Uncontrolled_Flow is countered by:

a) O.Policy_Enforce ensures that only authorised message protocols can be passed to a network
b) O.Policy_Enforce, O.Policy_Invoke and OE.Policy_Enforce ensure that messages can only be passed to a network on successful completion of Message Policy defined checks covering security labels, malicious or inappropriate content.

**T.Compromised_Flow Message Flow Compromised on Networks**
An authorised user or unauthorised person on one subscriber network, or intervening network, may attempt to send a valid subscriber message spoofing the source identity of another user, or replay a valid message from another user, eavesdrop on or modify messages from another user in transit.

T.Compromised_Flow is countered by:

a) O.Policy_Enforce, O.Policy_Invoke, and OE.Policy_Enforce ensure that only messages conforming to a Message Policy defined PKI status can be passed to a network.

**T.Unauthorised_Access Unauthorised Access to Message or TOE**
An authorised user or unauthorised person on a subscriber network or a network connected to a DMZ network may attempt to bypass CSDS policy enforcement, eavesdrop on or modify subscriber messages in transit through CSDS or interfere with CSDS data (Message Policies,

message queues, audit logs) by modifying CSDS security data or by exploiting ambiguities in the messaging standards or data types.

T.Unauthorised_Access is countered by:

a) O.IDAuth, OE.IDAuth, OE.ClearPoint_Support, OE.SPIF_Editor_Support and OE.Policy_Server_Support ensure that only authorised administrators can legitimately access TOE security data
b) OE.NoRemo prevents direct access to a Policy Server from subscriber networks
c) OE.DOS_Protection and OE.DMZ_Protection limit CSDS exposure to the required protocols
d) OE.ConFlo ensures that information flowing between the two subscriber networks cannot bypass a Policy Server
e) O.Policy_Enforce ensures that ambiguities in the messaging standards or data types cannot be exploited
f) OE.Policy_Distribution_Integrity protects Message Policies and SPIFs in transit between a remote ClearPoint, SPIF Editor, remote DSA and the DMZ network.

**T.Unaccountable_Actions** **Unaccountable Actions**

Authorised users, unauthorised persons or CSDS software components may not be accountable for their actions and attempts to compromise Message Policy and CSDS security.

T.Unaccountable_Actions is countered by:

a) O.IDAuth and OE.IDAuth ensure that authorised administrators are identified to the CSB2/TSOL platform prior to any other action
b) O.Policy_Enforce, as one of the mediation function checks referenced in Section 2.5.3, ensures that subscribers are identified before applying Message Policy, by identifying and validating all originator/recipient pairs per subscriber message
c) O.Auditing, OE.Accountability and OE.Auditing ensure that subscribers and authorised administrators are held accountable for their actions.

**T.Complexity** **Mis-Configuration of Message Policy**

Authorised administrators may inadvertently mis-configure Message Policy due to its complexity.

T.Complexity is countered by:

a) O.Management_Enforce provides an intuitive graphical user interface for administration of Message Policy, which eases the administration task involved in managing complex email policies, and ensures that TOE administrators are advised of Message Policy checks and actions that are to be enforced partly or wholly by external libraries
b) OE.DMZ_Separation ensures that policies meant for one direction of flow are not confused with those for the other direction of flow.

**T.Unauthorised_Admin** **Unauthorised Use of Administration Role**

Authorised administrators may exceed their authority by attempting to perform actions outside of their prescribed role.

T.Unauthorised_Admin is countered by:

a) O.IDAuth, OE.IDAuth, OE.ClearPoint_Support, OE.SPIF_Editor_Support and OE.Policy_Server_Support ensure that only authorised administrators may access the management functions of CSDS, CSB2, TSOL, boundary separation devices and packet firewalls

b) O.Management_Enforce, O.Management_Invoke and OE.SecFun provide CSDS, CSB2, TSOL, boundary separation devices and packet firewalls security management functions for authorised administrative roles

c) OE.ClearPoint_Support provides support libraries that enable the ClearPoint management interface to perform, via a ClearPoint external management subsystems, additional management operations to configure Policy Server external libraries.

d) OE.Access_to_PKI_Data restricts access to PKI Data, which enables assignment of users, to specific roles.

**T.Unpredictable** **Unpredictable Application of Message Policy**

CSDS software may perform unpredictable checks and actions due to failures in software or hardware or due to ambiguities in the messaging standards or data types, thus compromising the application of subscriber message policy.

T.Unpredictable is countered by:

a) O.Policy_Enforce prevents unpredictable checks and actions due to ambiguities in the messaging standards or data types

b) OE.SecSta ensures security is maintained during start-up or recovery from an interruption in CSDS Server service

c) OE.Prot_Against_Nature and OE.Prot_Agnst_Pwr_Fail protect the CSDS Server against natural disasters or power failures.

**T.Residual** **Release of Residual Information**

CSDS software may release in the current message residual information from previous messages due to a failure to clear storage resources between the processing of individual messages.

T.Residual is countered by:

a) O.Policy_Enforce ensures that residual information from previous messages is not released in the current message

b) OE.Residual_Info provides facilities to clear storage prior to reuse.

### 7.1.4 Policies

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

**P.Label**: **Secure Labelling Policy**

CSDS shall be suitable for use in an organisation that mandates, or accepts, use of secure formal message labelling conforming to [X.400], [STANAG 4406] or [S/MIME] standards and optionally to [X.841], or use of informal (text) message labelling in the message's Subject heading field or first line of text.

P.Label is met by:

a) O.Management_Enforce, O.Management_Invoke, OE.ClearPoint_Support and OE.SPIF_Editor_Support permits administrator selection of security labels and clearances in accordance with [X.400], [STANAG 4406] or [S/MIME] and optionally [X.841] standards

b) O.Policy_Enforce extracts and inserts security labels into messages in accordance with [X.400], [STANAG 4406] or [S/MIME] standards
c) When the X.841 LSL option is used, O.Policy_Enforce checks formal security label validity and domination by a specified clearance, translates a formal security label from one X.841 Security (Label) Policy to another and provides text rendition of a formal security label
d) O.Policy_Invoke invokes label checks in accordance with [X.841] and proprietary formal security label standards
e) OE.Policy_Enforce enforces label checks in accordance with proprietary formal security label standards.

P.Crypto: Cryptographic Standards and Algorithms
CSDS shall be suitable for use in an organisation that mandates, or accepts, use of secure messaging conforming to [S/MIME] standards and, as a minimum, the following cryptographic algorithms:

- Digital signature: RSA, any required key size, in accordance with [RFC 3447]; DSA, key sizes between 512 and 2048 bits inclusive, in accordance with [FIPS Pub 186]
- Symmetric encryption: AES, minimum 128 bit key size, in accordance with [RFC 3565] and [FIPS Pub 197]; Triple DES, minimum 112 bit key size, in accordance with [ANSI X9.52].
- Key generation: AES, minimum 128 bit key size, in accordance with [RFC 3565] and [FIPS Pub 197]; Triple DES, minimum 112 bit key size, in accordance with [RFC 3370] and [ANSI X9.52]
- Asymmetric encryption for distribution of symmetric keys: Diffie-Hellman, in accordance with [RFC 3370] and [RFC 3565]; RSA, in accordance with [RFC 3370] and [RFC 3565].

P.Crypto is met by:

a) O.Management_Enforce, O.Management_Invoke and OE.ClearPoint_Support permit administrator selection of cryptographic algorithms in accordance with S/MIME and relevant standards
b) O.Policy_Enforce extracts and inserts signatures and certificates into messages in accordance with S/MIME standards
c) O.Policy_Invoke invokes cryptographic algorithms in accordance with relevant standards
d) OE.Policy_Enforce enforces cryptographic algorithms in accordance relevant standards.

## 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.IDAuth | FIA_UAU.2X, FIA_UID.2X |
| O.Management_Enforce | FMT_MOF.1, FMT_MSA.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1 |
| O.Management_Invoke | FMT_SMF.1X |
| O.Auditing | FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SEL.1, FAU_STG.4X |
| O.Policy_Enforce | FDP_IFC.1, FDP_IFF.1, FMT_MSA.3X, FDP_LCK.2X |
| O.Policy_Invoke | FDP_IFC.1, FDP_IFF.1, FCS_COP.1X, FDP_LCK.1X, FDP_SPD.1X, FDP_TAO.1X, FDP_TCK.1X, FDP_VSF.1X |

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

O.IDAuth: Unique Identity and Authentication
The Policy Server must uniquely identify and authenticate the claimed identity of all authorised CSDS Server-mode Administrators before granting them access to Policy Server functions. The TOE must check the authenticity of all Message Policies and SPIFs downloaded to the TOE from a DSA.

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. FIA_UAU.2X ensures that Message Policies and SPIFs downloaded to the TOE may only be used if they are authenticated and associated with an appropriate authorised administrator.

O.Management_Enforce: Security Management Functions
The TOE must provide role based security management functions that permit authorised TOE administrators to manage the TOE security attributes and data. The TOE must provide a graphical interface which supports clear, consistent and accurate definition and review of those parts of the Message Policy enforced by the Policy Engine and the optional X.841 LSL external library. The TOE must advise TOE administrators of Message Policy checks and actions that are enforced partly or wholly by external libraries.

FMT_SMR.1 ensures that the TOE maintains two, optionally three, distinct authorised TOE administrator roles for Policy Engine administration functions (CSDS Directory-mode Administrator, CSDS Server-mode Administrator and (optionally) X.841 Security (Label) Policy Administrator). The administration functions available to an administrator acting in the role of a CSDS Server-mode Administrator depend on the Administrator Privileges assigned to the administrator. FMT_MOF.1 provides role specific security functions to stop/re-start a Policy Engine. FMT_MSA.1, FMT_MTD.1 and FMT_SMF.1 provide role specific security functions to manage Policy Server configuration and Policy Engine queues, to select and administer a Message Policy and optionally to administer X.841 Security (Label) Policy. FMT_SMF.1 also provides security functions to manage PKI data on Policy Servers, ClearPoint Management Stations and SPIF Editor Platforms, which are also role specific, but with administrators that are identified and authenticated, and roles that are assigned, by the underlying platforms rather than the TOE.

**O.Management_Invoke:** **Invoke External Management Functions**
The TOE must correctly invoke those security management functions that permit authorised TOE administrators to manage Message Policy attributes required by the Policy Server external libraries listed in Section 2.6.

FMT_SMF.1X ensures that ClearPoint external management functions are correctly invoked.

**O.Auditing:** **Auditing of Message Flows and Administrator Actions**
The TOE must provide the capability to record all subscriber message flows and their association with the originator and recipients. The TOE must provide the capability to record TOE administrator selectable details of the application of Message Policy on subscriber message flows. The TOE must record the security relevant actions of TOE administrators. The TOE must provide the capability for TOE administrators to view audit records.

FAU_GEN.1and FAU_GEN.2 ensure that all subscriber message transactions and all actions performed by authorised TOE administrators can be configured to generate audit records. FAU_SEL.1 provides the capability for TOE administrators to select for audit details of the application of Message Policy on subscriber message flows. FAU_SAR.1 provides the capability for TOE administrators to view audit records. FAU_STG.4X ensures that no audit records of subscriber message transactions are lost if the audit logs are full.

**O.Policy_Enforce:** **Mediation of Flow of Information**
The TOE must enforce the subscriber message mediation functions that are provided by the Policy Engine and the optional X.841 LSL external library, as defined in Section 2.5.3.

FDP_IFC.1 and FDP_IFF.1 enforces all subscriber message mediation functions that are provided by the Policy Engine and the optional X.841 LSL external library, as defined in Section 2.5.3. FDP_LCK.2X enforces the optional X.841 security label checks and actions. FMT_MSA.3X ensures that no subscriber message flow is permitted prior to the selection and activation of a Message Policy.

**O.Policy_Invoke:** **Invocation of Policy Check and Actions**
The TOE must correctly invoke those parts of the Message Policy defined checks and actions that are provided by the Policy Server external libraries listed in Section 2.6.

FDP_IFC.1, FDP_IFF.1, FCS_COP.1X, FDP_LCK.1X, FDP_SPD.1X, FDP_TAO.1X, FDP_TCK.1X and FDP_VSF.1X ensure that those parts of the Message Policy defined checks and actions required by the active Message Policy for each subscriber message are correctly invoked.

#### 7.2.1.2 IT Environment SFRs meet the IT Environment Security Objectives

As stated in Section 5.3.1, the Policy Server relies on SFRs specified in Sections 5.3.2 and 5.3.3 which define the requirements for cryptographic operations and associated key management, formal security label checking operations, spam detection operations, textual analysis operations, data type checking (including macro detection) operations, and virus scanning to be supplied, respectively, by several external libraries: a cryptographic subsystem; a formal security label subsystem; spam detection subsystems; textual analysis subsystems; data type checking subsystems; VS subsystems. 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, and 5.3.3. The justification that the identified SFRs are required and suitable to meet the IT Environment objective is self-evident.

As stated in Section 5.3.1, ClearPoint relies on SFRs specified in Section 5.3.2, Paragraph 5.3.3.1 and Section 5.3.4, which define the requirements for cryptographic operations, associated key management, label checking operations and ClearPoint external management operations to be supplied, respectively, by the external libraries: a cryptographic subsystem and a cryptographic library accessed through the Microsoft CryptoAPI; a formal security label subsystem; ClearPoint external management subsystems. 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 Section 5.3.2, Paragraph 5.3.3.1 and Section 5.3.4. The justification that the identified SFRs are required and suitable to meet the IT Environment objective is self-evident.

As stated in Section 5.3.1, SPIF Editor relies on SFRs specified in Section 5.3.2 which define the requirements for cryptographic operations and associated key management to be supplied by the cryptographic subsystem external library. 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 Section 5.3.2. The justification that the identified SFRs are required and suitable to meet the IT Environment objective is self-evident.

As specified in Section 5.3.1, the Policy Server, ClearPoint and SPIF Editor rely on the use of the cryptographic subsystem digital signature operations to verify the integrity of Message Policies and SPIFs received from a remote SPIF Editor, ClearPoint in Directory-mode or DSA (via a DSA on the DMZ network). This is expressed as the IT environment security objective OE.Policy_Distribution_Integrity, 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 and shown in Table 7.3.

Table 7.3 – CSDS Security Objectives for the IT Environment to Sections 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 Sections 5.3.2, 5.3.3, 5.3.4 and 5.3.5 |
|---|---|
| OE.Policy_Enforce | FCS_COP.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FDP_LCK.3X, FDP_SPD.2X, FDP_TAO.2X, FDP_TCK.2X, FDP_VSF.2X. |
| OE.Policy_Distribution_Integrity | FPT_ITI.1 |
| OE.ClearPoint_Support | FCS_COP.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FDP_LCK.3X, FMT_SMF.1 |
| OE.SPIF_Editor_Support | FCS_COP.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.4 |
| OE.Policy_Server_Support | FCS_COP.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FDP_LCK.3X |

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_PKI_Data | O.MANDATORY_ACCESS, O.DISCRETIONARY_ACCESS, O.ENFORCEMENT |
| OE.Residual_Info | O.RESIDUAL_INFORMATION |
| OE.Accountability | O.AUDITING |
| OE.Auditing | O.AUDITING |

As stated in Section 5.3.1, ClearPoint relies on selected SFRs from Microsoft Windows' implementation of the SFRs required to comply with the [CAPP] protection profile. SPIF Editor relies on selected SFRs from Microsoft Windows', Solaris' or Linux's implementation of the SFRs required to comply with the [CAPP] protection profile. Table 7.6 provides a mapping between the CSDS security objectives for the IT environment and the relevant [CAPP] security objectives, thus providing an implicit mapping to the relevant Microsoft Windows, Solaris and Linux security functional requirements (SFRs).

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

Table 7.6 – CSDS Security Objectives for the IT Environment to [CAPP] Security Objective Mapping

| CSDS Security Objectives for the IT Environment | TSOL TOE security objectives |
|---|---|
| OE.IDAuth | O.AUTHORISATION |
| OE.SecFun | O.MANAGE, O.DISCRETIONARY_ACCESS, O.ENFORCEMENT |
| OE.Access_to_PKI_Data | O.DISCRETIONARY_ACCESS, O.ENFORCEMENT |

As specified in Section 5.3.1, the TOE relies on the IT environment to protect CSDS components 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 FAU_STG.4X component is explicitly stated. It is a modified version of the [CC] Part 2 component FAU_STG.4 that is necessary because the requirement is not applicable to all audit events but restricted to subscriber message transaction events. It is hierarchical to no other component and has one dependency, FAU_STG.1, met by the IT environment. The EAL4 assurance requirements are fully applicable to FAU_STG.4X.

The SFR FCS_COP.1X component is explicitly stated. It is an additional component 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 component 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, optionally FDP_LCK.2X, met by the TOE or FDP_LCK.3X, met by the IT environment. The EAL4 assurance requirements are fully applicable to FDP_LCK.1X.

The SFR FDP_LCK.2X component is explicitly stated. It is an additional component that is necessary because it specifies the requirement to enforce formal security label checking operations using Security (Label) Policy information in X.841 SPIFs. It is hierarchical to no other component and has no dependencies. The EAL4 assurance requirements are fully applicable to FDP_LCK.2X.

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

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

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

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

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.

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

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.

SFR FMT_SMR.1.2 is refined by replacing the term “users” with the term “TOE Administrators”, as only TOE Administrators are associated with roles by the TOE.

Similarly, in the CC Class FDP description, the term “user” is replaced with the term “Subscriber”, as the policy for information flow control applies to subscriber data only.

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 7.7 demonstrates that all the TOE requirement dependencies are met or provides an explanation of why the dependency is inappropriate.

Table 7.7 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 a subscriber message transaction, where the user causing the event, identified by the Policy Engine, is the subscriber that sends the message. |
| FAU_SAR.1 | FAU_GEN.1 |
| FAU_SEL.1 | FAU_GEN.1. The dependency on FMT_MTD.1 is met by FMT_MSA.1, because FAU_SEL.1 only applies to message transaction events, and these are selected using FMT_MSA.1 as a secondary action applied to individual Message Policy rules (see Annex A). |
| FAU_STG.4X | FAU_STG.1. This dependency is met by the IT environment. |
| 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 or FDP_LCK.3X. The dependency on FDP_LCK.2X is met by the TOE, when the X.841 LSL option is included. The dependency on FDP_LCK.3X is met by the IT environment. |
| FDP_LCK.2X | – |
| FDP_SPD.1X | FDP_SPD.2X. This dependency is met by the IT environment. |
| FDP_TAO.1X | FDP_TAO.2X. This dependency is met by the IT environment. |
| FDP_TCK.1X | FDP_TCK.2X. This dependency is met by the IT environment. |
| FDP_VSF.1X | FDP_VSF.2X. This dependency is met by the IT environment. |

| Requirement | Dependencies |
|---|---|
| FIA_UAU.2X | FCS_COP.1X |
| FIA_UID.2X | FCS_COP.1X |
| FMT_MOF.1 | FMT_SMF.1, FMT_SMR.1 |
| FMT_MSA.1 | FDP_IFC.1, FMT_SMF.1, FMT_SMR.1 |
| FMT_MSA.3X | FMT_MSA.1 |
| FMT_MTD.1 | FMT_SMF.1, FMT_SMR.1 |
| FMT_SMF.1 | – |
| FMT_SMF.1X | 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 7.7 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 7.8 demonstrates that all the IT environment requirement dependencies are met or provides an explanation of why the dependency is inappropriate.

Table 7.8 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.Access_to_PKI_Data) |

| Requirement | Dependencies |
|---|---|
| FCS_CKM.2 | FCS_CKM.1, FCS_CKM.4, FMT_MSA.2 (Met instead by OE.Access_to_PKI_Data) |
| FCS_CKM.4 | FCS_CKM.1, FMT_MSA.2 (Met instead by OE.Access_to_PKI_Data) |
| FCS_COP.1 | FCS_CKM.1, FCS_CKM.4, FMT_MSA.2 (Met instead by OE.Access_to_PKI_Data) |
| For Label Checking Operations | |
| FDP_LCK.3X | – |
| For Spam Detection Operations | |
| FDP_SPD.2X | – |
| For Textual Analysis Operations | |
| FDP_TAO.2X | – |
| For Data Type Checking Operations | |
| FDP_TCK.2X | – |
| For Virus Scanner Operations | |
| FDP_VSF.2X | – |
| For Specification of Management Functions | |
| FMT_SMF.1 | – |
| For Inter-TSF Detection of Modification | |
| FPT_ITI.1 | FCS_COP.1 |

As can be seen from Table 7.8 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 in the TOE for which a Strength of Function claim would be appropriate, 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 7.9 demonstrates that the combination of specified TOE security functions work together to satisfy the TOE security functional requirements.

Table 7.9 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-2 |
| FAU_SAR.1 | MANAGE-5 |
| FAU_SEL.1 | MANAGE-13 |
| FAU_STG.4X | AUD-3 |
| FCS_COP.1X | CRYPTO-1 |
| FDP_IFC.1 | CSB2-1, QUEUE-1, POLICY-2 to POLICY-12 |
| FDP_IFF.1 | CSB2-1, QUEUE-1, POLICY-2 to POLICY-12 |
| FDP_LCK.1X | LABEL-1 |
| FDP_LCK.2X | LABEL-2 |
| FDP_SPD.1X | SPAM-1 |
| FDP_TAO.1X | TEXT-1 |
| FDP_TCK.1X | TYPE-1, MACRO-1 |
| FDP_VSF.1X | VS-1 |
| FIA_UAU.2X | I&A-1 to I&A-5 |
| FIA_UID.2X | I&A-1 to I&A-5 |
| FMT_MOF.1 | MANAGE-4, MANAGE-10, MANAGE-12 |
| FMT_MSA.1 | AC-1, MANAGE-11 to MANAGE-14 |
| FMT_MSA.3X | POLICY-1 |
| FMT_MTD.1 | AC-1, MANAGE-4 to MANAGE-10 |
| FMT_SMF.1 | MANAGE-1 to MANAGE-14 |
| FMT_SMF.1X | MANAGE-13 |
| 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-2 ensures that records of auditable events contain the identity of the user that initiated the event.

FAU_SAR.1 requires that administrators are able to read audit records. MANAGE-5 enables CSDS Server-mode Administrators having Audit Log Viewing administrator privilege to view the contents of audit log files.

FAU_SEL.1 requires that administrators are able to select auditable events associated with specific Message Policy rules and relationships. MANAGE-13 enables CSDS Server-mode Administrators having Message Policy Administration administrator privilege and CSDS Directory-mode Administrators to select for audit message transaction events associated with specific Message Policy rules and relationships.

FAU_STG.4X requires that message processing is stopped if the audit trail is full. AUD-3 prevents further message processing if the Policy Engine audit log is full.

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 cryptographic operations provided as a vendor specific library.

FDP_IFC.1 requires that all messages are subject to the CSDS Message Flow Control Policy. CSB2-1 configures CSB2 channels for each direction of subscriber message flow and installs a Policy Server in each VET compartment. QUEUE-1 moves inbound and outbound messages between CSB2 and CSDS queues, maintaining the correct association, depending on the direction of subscriber message flow. POLICY-2 to POLICY-12 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. CSB2-1 configures CSB2 channel for each direction of subscriber message flow and installs a Policy Server in each VET compartment. QUEUE-1 moves inbound and outbound messages between CSB2 and CSDS queues, maintaining the correct association, depending on the direction of subscriber message flow. POLICY-2 to POLICY-12 ensure that the Message Policy is applied to all subscriber messages.

FDP_LCK.1X requires that calls to label checking operations performed by the IT environment are properly formed. LABEL-1 calls appropriate label checking operations correctly.

FDP_LCK.2X requires that formal security label checking operations are enforced using Security (Label) Policy information in X.841 SPIFs, when the optional X.841 LSL external library is included in the Policy Server. LABEL-2 enforces operations which check that a given formal security label is valid, that a formal security label is dominated by a specified clearance, maps a given formal security label from one X.841 Security (Label) Policy to another and renders a given formal security label into text.

FDP_SPD.1X requires that calls to spam detection operations performed by the IT environment are properly formed. SPAM-1 calls appropriate spam detection operations correctly.

FDP_TAO.1X requires that calls to textual analysis operations performed by the IT environment are properly formed. TEXT-1 calls appropriate textual analysis operations correctly.

FDP_TCK.1X requires that calls to data type checking (including macro detection) operations performed by the IT environment are properly formed. TYPE-1 calls appropriate data type checking operations correctly. MACRO-1 calls appropriate macro detection operations correctly.

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

FIA_UAU.2X requires that all users of the TOE are authenticated. I&A-1 to I&A-5 identifies and authenticates users using individual authenticated certificates.

FIA_UID.2X requires that all users of the TOE are identified. I&A-1 to I&A-5 identifies and authenticates users using individual authenticated certificates.

FMT_MOF.1 requires specific functions to disable and enable the functions of subscriber message flow. MANAGE-4, MANAGE-10 and MANAGE-12 provide these functions by enabling stop/re-start of a Policy Engine.

FMT_MSA.1 requires restriction on specific functions for specific roles to manage Message Policy and SPIFs. MANAGE-11 to MANAGE-14 provide these functions and AC-1 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. POLICY-1 provides this function.

FMT_MTD.1 requires restriction on specific functions for specific roles to manage Policy Server data and to release, non-deliver or discard subscriber messages from MANUAL queues. MANAGE-4 to MANAGE-10 provide these functions and AC-1 restricts them to the defined roles.

FMT_SMF.1 requires specific functions to manage Policy Server PKI data, ClearPoint PKI data, SPIF Editor PKI data, Message Policies, SPIFs and Policy Server data. MANAGE-1 to MANAGE-14 provide these functions.

FMT_SMF.1X requires that calls to external management functions performed by the IT environment are properly formed. MANAGE-13 calls appropriate management functions correctly.

FMT_SMR.1 requires that there are defined roles associated with users. AC-1 ensures that all TOE Administrators 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
## Message Policy

Message Policy is a distinct configuration of the sets of subscribers, originator/recipient pairs (relationships), rules and attributes that, when loaded into an instantiation of the Policy Engine (i.e. made the active Message Policy), mediates the flow of subscriber messages in accordance with 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 Policy may be defined and modified by a CSDS Server-mode Administrator having Message Policy Administration administrator privilege or a CSDS Directory-mode Administrator, referred to subsequently in this annex as “administrator”.

Message Policy comprises:

- Policy tree
- Policy relationships
- Policy rules
- Attributes.

### Policy Tree

A policy tree consists of a hierarchy of objects defined for elements of the Company and World networks and organisations. It comprises by default a root domain for Company and a root domain for World. An administrator can define under each root further objects of type domain, group and user (subscriber). Further domains, groups and users may be defined under domains and groups, but not under users. It is not necessary to define objects in the hierarchy for each real user, group and domain in each organisation: it is sufficient just to create objects in the hierarchy where exceptional policy is required, and assign all subscribers who are to have identical policy to the same object in the hierarchy.

### Policy Relationships

A policy relationship is a relationship from an object in a domain hierarchy (Company or World) representing a message originator to an object in a domain hierarchy (Company or World) representing a message recipient, together with the associated policy rules for that relationship. The policy relationship represents the originator/recipient pair against which email will be compared to determine the policy rules to be applied. A policy relationship is unidirectional.

A policy relationship may be from an object in the Company domain hierarchy to an object in the World domain hierarchy, from an object in the World domain hierarchy to an object in the Company domain hierarchy, from an object in the Company domain hierarchy to an object in the Company domain hierarchy, or from an object in the World domain hierarchy to an object in the World domain hierarchy. In the latter two cases, a relationship may be from an object to itself.

Every Message Policy specifies at least one policy relationship for each of these four cases: the initial default policy relationships for the Company and World root domains. Thereafter, an administrator may define further policy relationships. For each email received by a Policy Server, the policy relationship that most closely matches the email's originator/recipient pair is found and the associated policy rules applied.

### Policy rules

Policy rules are defined for each policy relationship defined in the Message Policy. An initial default set of policy rules is defined on each of the four default policy relationships between the Company and World root domains. (The default set of policy rules for each relationship is defined by the Message Policy template selected by an administrator when first creating a new Message Policy. CSDS is initially installed with default templates having "open" and "closed" policies, including ones for general use, ones for conformance to [STANAG 4406] and ones for conformance to [ACP 145]. "Open" allows all email to pass between the root domains; "closed" non-delivers all email).

For each new policy relationship created, the associated policy rules are initially inherited from those of the policy relationship at the next higher level in the hierarchy. The administrator may refine individual policy rules in a policy relationship, thus breaking the inheritance chain for those rules (and, if required, may later unrefine rules).

Policy rules are grouped, and each group of policy rules may be enabled or disabled. The Policy Server applies only policy rules that are in a group that is enabled in the policy relationship. This allows policy rules to be defined at one level of the hierarchy but activated at another level.

The available policy rule groups and policy rules are dependent on the installed software licence key, which will activate a selection, or (unusually) all, of the following:

**Policy Rule Group**
- **Policy Rule**

For all E-mail on this relationship
- If unable to decode
- If non-fatal protocol violation

Unsupported protocol extensions
- Envelope extensions
- Content extensions
- Certificate/CRL extensions
- S/MIME CMS attributes

Unsupported MIME encoding
- MIME transfer encoding not supported
- MIME character set not supported

Message Type
- X.400 Message
- X.400 Delivery Report
- X.400 Non-Delivery Report
- X.400 Receipt Notification
- X.400 Non-Receipt Notification
- X.400 Other Notification
- X.400 Probe
- X.400 Unsupported Content Type

- SMTP Message
- SMTP Delivery Status Notification
- SMTP Message Disposition Notification

Returned Content

X.400 Precedence (Priority)
- Override
- Flash (Urgent)
- Immediate
- Priority (Normal)
- Routine
- Deferred (Non-urgent)

X.400 Content Types
- <X.400 content type rules>

X.400 Body Part Types
- <X.400 body part rules>

SMTP Headers
- <SMTP header rules>

MIME Media Types
- <MIME media type rules>

Size Restriction
- Threshold

Size Restriction per Precedence
- Override
- Flash (Urgent)
- Immediate
- Priority (Normal)
- Routine
- Deferred (Non-urgent)

Enforce Signature/Encryption *
- Incoming clear text message
  - if disallowed
- Incoming signed message
  - if disallowed
- Incoming encrypted message
  - if disallowed
- Incoming signed encrypted message
  - if disallowed
- Signature cannot be verified
- Signer is not originator
- Content which cannot be decrypted

Security Labelling **
- If unlabelled
- Assign Default Label
- If labels mismatch
- <Security Clearances>
- If security label not cleared

- First Line Labelling
  - <FLOT rules>
  - Action if no match or absent
- Subject Labelling
  - Subject label
  - If label exceeded
  - If label below or matched
  - If label is bad
- Spam Filtering ***
  - <spam rules>
- Attachment Data Type Filtering ***
  - <data type rules>
  - Container which cannot be decomposed
  - Unable to extract all files from container
  - If container content is modified
  - Attachment data corrupt
  - Attachment data format warnings
  - Wrong file extension
  - Wrong content GUID
  - Wrong MIME type
  - Wrong X.400 Body Part Type
- Macro Filtering ***
  - <macro rules>
  - Certify content is free of macros
- Virus Scanning ***
  - If a virus is detected
  - If virus cannot be cleaned
  - If virus scan fails
  - Certify content is free of viruses
- Textual Analysis ***
  - <lex rules>
- Message Modification
  - Add text annotation
  - Add Security Label
  - Add First Line Label
  - Add Subject Label
  - Add SMTP Header
  - Add Subject Information Code
  - MIME Multipart Preambles
  - MIME Multipart Epilogues
- Security Label Modification **
  - Map outgoing Security Labels
    - if mapping fails
  - Output label position
- Signature/Encryption Modification *
  - Signature algorithms
  - Key exchange algorithms

Encryption algorithms
Output signature format
Include signer certificate
Output clear text messages
    if conversion fails
Output signed messages
    if conversion fails
Output encrypted messages
    if conversion fails
Re-sign message
    if signed content modified
Sign as originator or gateway
    if no key for originator
Re-encrypt message
Outer signature of triple-wrap

Notifications
Send to originator
Send to administrator
Send to recipient
Send to PAA

Notes on policy rule groups and policy rules:

* Policy rules in these policy rule groups are mainly enforced by the TSF, but make use of cryptographic operations provided by the external cryptographic subsystem library.

** Policy rules in these policy rule groups are enforced by the TSF if the optional X.841 formal security label subsystem library is installed. Otherwise, their enforcement depends on results from an alternative formal security label subsystem which is external to the TOE. The application of the results to the message is within the scope of the TSF.

*** The enforcement of policy rules in these policy rule groups depends on results from appropriate libraries which are external to the TOE. The application of the results to the message is within the scope of the TSF.

Each policy group and rule may comprise one or more specific checks (the outcome of which will result in one of the available primary actions for the rule) and specific actions. It may also be associated with secondary actions that may trigger depending on the results of the checks.

Each policy rule that specifies an action may also specify an additional policy rule set to be applied only when it is triggered and an additional policy rule set to be applied only when the rule is applicable but is not triggered. A policy rule in an additional policy rule set may itself specify further additional policy rule sets. This enables any policy rule to be made conditional on the result of applying any sequence of other policy rules.

Primary actions available are:

- Pass-through message
- Cleanse message element
- Delete message element

- Queue for manual intervention in a named MANUAL queue
- Non-deliver message
- Discard message.

Secondary actions available are:

- Archive Inbound (on entry to Policy Engine)
- Archive Outbound (on exit from Policy Engine)
- Audit (details of message processing associated with this policy rule)
- Annotate message with text (e.g. warn recipient that message contains macro)
- Inform (designated groups and individuals of processing associated with this policy rule)
- Invoke an additional policy rule set if the rule is triggered
- Invoke an additional policy rule set if the rule is not triggered.

### Attributes

This section of the Message Policy contains definitions of attributes used in policy rules. The categories of attributes available are:

- Data types
- MIME media types
- X.400 content types
- X.400 body parts
- SMTP Headers
- Spam rules
- Textual analysis rules
- Annotations and Notifications (text fragments)
- Subject labels
- List of named MANUAL queues (in addition to default queues named “hold” and “quarantine”).

# Annex B
## Policy Server Configuration Data

Policy Server Configuration Data is defined for each Policy Server by a CSDS Server-mode Administrator having Policy Server Configuration Administration administrator privilege using ClearPoint in Server-mode, and comprises:

- Policy Server identity
- X.400 & SMTP address identities (Server, PAA, Administrator)
- message precedence attributes (expiry periods, thread-pool settings)
- attributes to control internally generated emails (sign/not-sign, email audit-logs)
- identification of external libraries for data type recognition, textual analysis, virus scanning and spam detection
- audit log attributes (preserve period, roll-over period, warning message water-marks)
- archive control attributes (preserve period, roll-over period).

# Annex C
## Rationale for alternative ClearPoint external management subsystems

ClearPoint accesses the installed ClearPoint external management subsystems through a well-defined API, which is fully specified in terms of effects, exceptions and error messages.

The CSDS TOE was evaluated using each of the ClearPoint external management subsystems identified in Table 2.2 in Section 2.7.1. However the scope of the TOE is such that the focus of the evaluation, with respect to the subsystem, was on the TOE invoking use of the subsystem and acting on responses received from it. The API to the subsystems was evaluated in the course of this activity.

The evaluated CSDS TOE can be used in conjunction with a number of ClearPoint external management subsystem options. Whilst the ClearPoint external management 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 ClearPoint external management subsystems that it considers reputable.
- Testing to exercise the use of each ClearPoint external management subsystem in conjunction with CSDS. This testing includes authentication of CSDS users by the Administration Service and full testing of the CSDS Message Flow Control Policy using various configurations of the Message Policy, and fully exercising the subsystem API. 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 D
## Rationale for alternative cryptographic subsystem

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

The CSDS TOE was evaluated using each of the cryptographic subsystems identified in Table 2.2 in Section 2.7.1. 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 API 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 cryptographic subsystem options. Whilst the cryptographic 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 cryptographic subsystems that it considers reputable.
- Testing to exercise the use of each cryptographic subsystem in conjunction with CSDS. This testing includes authentication of CSDS users by the Administration Service and full testing of the CSDS Message Flow Control Policy using various configurations of the Message Policy, and fully exercising the subsystem API. 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 E
## Rationale for alternative formal security label subsystem

CSDS accesses the installed formal security label subsystem through a well-defined API, 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 2.02.05 and the 'Null LSL for CSDS' Pkg Vn 2.01.36 formal security label subsystems. The former is within the scope of this TOE and the latter is not within the scope of this TOE. 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 API 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 formal security label subsystem options. Whilst the formal security label subsystem itself may, or may not, be within the scope of this TOE, Clearswift undertakes a number of activities to ensure provision of quality customer solutions which include:

- Use of formal security label subsystems that it considers reputable.
- Testing to exercise the use of each formal security 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 API. 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 F
## Rationale for alternative data type recognition subsystems

CSDS accesses the installed data type recognition subsystems through a well-defined API, which is fully specified in terms of effects, exceptions and error messages.

The CSDS TOE was evaluated using each of the data type recognition subsystems identified in Table 2.2 in Section 2.7.1. 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 API to the subsystems was evaluated in the course of this activity.

The evaluated CSDS TOE can be used in conjunction with a number of data type recognition subsystem options. Whilst the data type recognition 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 [type] recognition subsystems that it considers reputable.
- Testing to exercise the use of each data type recognition 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 API s for data type recognition and conformance, decomposition, text extraction, macro detection and re-composition. 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 G
## Rationale for alternative textual analysis subsystems

CSDS accesses the installed textual analysis subsystems through a well-defined API, which is fully specified in terms of effects, exceptions and error messages.

The CSDS TOE was evaluated using each of the textual analysis subsystems identified in Table 2.2 in Section 2.7.1. 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 API to the subsystems was evaluated in the course of this activity.

The evaluated CSDS TOE can be used in conjunction with a number of textual analysis subsystem options. Whilst the textual analysis 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 textual analysis subsystems that it considers reputable.
- Testing to exercise the use of each textual analysis 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 API. 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 H
## Rationale for alternative spam detection subsystems

CSDS accesses the installed spam detection subsystems through a well-defined API, which is fully specified in terms of effects, exceptions and error messages.

The CSDS TOE was evaluated using each of the spam detection subsystems identified in Table 2.2 in Section 2.7.1. 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 API to the subsystems was evaluated in the course of this activity.

The evaluated CSDS TOE can be used in conjunction with a number of spam detection subsystem options. Whilst the spam detection 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 spam detection subsystems that it considers reputable.
- Testing to exercise the use of each spam detection 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 API. 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 I
## Rationale for alternative Virus Scanner subsystems

CSDS accesses the installed VS subsystems through a well-defined API, which is fully specified in terms of effects, exceptions and error messages.

The CSDS TOE was evaluated using each of the VS subsystems identified in Table 2.2 in Section 2.7.1. Each subsystem uses a VS filter that 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 a number of optional VS subsystems. Whilst the VS 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 VS filters that it considers reputable.
- Testing to exercise the use of each VS 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 API. 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 J
## Rationale for alternative CSB2/TSOL Platforms

It is asserted that use of the CSDS TOE with a future assurance maintained derivative of CSB2 (on specified version(s) of TSOL) would involve only a low risk of the security of the TOE being undermined.

This is based on the following rationale:

- the CSDS TOE makes straightforward use of CSB2 interfaces (associated only with CSB2 queues and VET compartments)
- the CSDS TOE uses standard Solaris programming interfaces and functions (e.g. file management and syslog) that are designed to be consistent between different Trusted Solaris 8 derivatives
- Clearswift programming standards would ensure that these interfaces and functions are used consistently throughout the CSDS and CSB2 TOEs, and this usage would be tested under the assurance maintenance of CSB2.

# Annex K
## Rationale for alternative ClearPoint Platforms

It is asserted that use of the CSDS TOE with ClearPoint installed on future upwards compatible versions of Internet Explorer and alternative versions of Microsoft Windows operating systems would involve only a low risk of the security of the TOE being undermined.

This is based on the following rationale:

- ClearPoint uses standard Internet Explorer and Windows programming interfaces and functions that are designed to be consistent between different versions
- Clearswift programming standards would ensure that these interfaces and functions are used consistently throughout ClearPoint
- ClearPoint's only security critical dependency on the ClearPoint platform is for the protection of the CSDS Server-mode Administrators' and CSDS Directory-mode Administrators' private keys, which may be protected using Windows security functions, or other alternatives (e.g. storage on a smart card).

# Annex L
## Rationale for alternative SPIF Editor Platforms

It is asserted that use of the CSDS TOE with SPIF Editor installed on future upwards compatible versions of Java conformant JVM and alternative versions of Microsoft Windows, Linux and Solaris operating systems would involve only a low risk of the security of the TOE being undermined.

This is based on the following rationale:

- SPIF Editor uses standard JVM, Windows Linux and Solaris programming interfaces and functions that are designed to be consistent between different versions
- Clearswift programming standards would ensure that these interfaces and functions are used consistently throughout SPIF Editor
- SPIF Editor's only security critical dependency on the SPIF Editor Platform is for the protection of the X.841 Security (Label) Policy Administrator's private key, which may be protected using the platform OS security functions, or other alternatives (e.g. storage on a smart card).