AUSTRALIAN SECURITIES & INVESTMENTS COMMISSION

EDGE INTERNET TRANSPORT LAYER

APPLICATION COMMUNICATION PROTOCOL

SPECIFICATIONS

Version 1.03

27 January 2016

CONTENTS

1. INTRODUCTION

1.1 Background

This document specifies communications protocols at the application communications level for applications using the Internet to lodge documents electronically with the Australian Securities & Investments Commission (ASIC) EDGE Electronic Lodgement System. This is known as the EDGE Internet interface (EII).

This EDGE Internet interface is specified at two levels:

- the presentation level, defined in this document, which describes the Application Communication Protocol (ACP) required to support conversations at the higher application level. Software developers will need this specification to be able to write the supporting software for any applications using the EDGE Internet interface. This level corresponds to the Open Systems Interconnection (OSI) reference model Presentation Layer, layer 6.

- the application level, defined in "EDGE Electronic Lodgement System Document Messages Specification", which defines the layout and content of application service request and reply messages. Software developers will need this specification to be able to write programs supporting specific application queries and services, such as e.g. a Company Incorporation. This level corresponds to the OSI Application Layer, layer 7.

The lower layers 1 - 4 of the OSI model are not described here. They are covered by the various Intenet RFCs and standards defining Internet communications.

1.2 EDGE DIS legacy system

The EII server provides transport services between a client system and the EDGE Document Interchange System (DIS). Consequently, developers of systems using this interface must also be familiar with the DIS features documented in the EDGE Document Interchange System Interface Specification. In particular, developers must be familiar with the function, naming conventions and content layout of report files produced by the DIS system, such as the DIS Transmission Report and Validation Report files.

The DIS system supports file transfer using X.25. The EII server is designed to provide client software with an easy to use TCP/IP based transport, shielding the protocol from most of the complexities of the DIS.

1.3 Document Overview

This document specifies communications protocols for EDGE Internet interface. Specifically, it includes:

- TCP/IP socket connection by the client application to the EDGE Internet Server (EIS).
- protocol stack used for communication and security.

It does not include hardware and low-level protocols required to support TCP/IP connectivity between the client and the EIS. In other words, it assumes a TCP/IP link exists.

EIS clients are able to obtain services by establishing an HTTP/SSL v3 (without client certificates) TCP/IP socket connection with the EDGE Internet server and sending service requests to the server. Data is sent half-duplex in both directions as discrete messages using a stripped-down SMTP protocol. Authentication is via EDGE userid/password as encrypted by SSL, and various X.509 certificates at the application layer (not at the SSL layer).

1.4 Other Relevant Documentation

EDGE specifications are available for download from **"http://www.asic.gov.au/api".**

Publicly available documentation of the ASIC's EDGE electronic lodgement system is listed in the Document Summary document in these specifications.

The ASIC may prepare other specifications and directions from time to time. They will be distributed to registered software developers.

1.5 Where to get help

Refer to the Documentation Summary specification.

2. PROTOCOL STACK

2.1 Overview

Conversations consist of a series of synchronous conversational messages. After connection and standard SSL handshake, conversations are then initiated by the client and continue in a simple client/server fashion, with each end waiting for reply or timeout before proceeding or ending.

The data transfers which make up the conversations are best understood using layering to separate out the various types of message.

There are considered to be several layers involved. Going from lowest to highest, these are:

- transport layer - TCP/IP
- security layer - SSL v3
- transport message layer - SMTP subset
- application session message layer - messages sent by SMTP.
- application message layer - EDGE messages.

2.2 Protocol Layers

2.2.1 Transport Layer

Client applications will connect to the EIS via a specified TCP/IP port on an EIS host. The specific host names and port number will be advised when the client has completed trading agreement prerequisites.

Software developers should use the host name provided and use Internet DNS services to translate this to the host IP address for every client session. In the future the actual IP address of the EIS may change due to reconfiguration and the use of failover and load balancing measures. Client software should not use hardcoded IP addresses.

ASIC will introduce fault tolerant failover measures during 2000. These measures will consist of providing two hostnames instead of one. Each hostname will connect to a specific backend EDGE mailbox, so developers and clients must be aware that if they switch EIS hosts (and hence EDGE mailbox) then the mailbox contents will not be the same. Each EIS is tied to a specific mailbox, and report files produced in response to lodged documents are sent only to the mailbox which received the document.

For further information on this topic, see the chapter titled “Application Level Control”

2.2.2 Security Layer

SSL v3 without client certificates is required using any SSL package that software developers choose to use. Suggested packages are described elsewhere in the EDGE specifications.

Developers are warned that it is up to them to operate the SSL protocol securely. This means:

- client packages should verify the server certificate signature against the CA certificate of the issuer, to guarantee that the chain of trust is intact.
- client packages should verify that the server certificate distinguished name is the name of the EIS server as advised by the EDGE Systems team to developers.

The Certificate Authority (CA) X.509 certificates used to issue the server certificates used by the EDGE Internet Servers are published in a place where developers and users can retrieve them. This allows verification of the security of their EIS connection, by checking that the server they are connected to is using a certificate issued by a trusted CA. For production, clients can also retrieve the same CA certificate from the web site of the CA.

The CA certificate can be obtained from ASIC's website identification by typing in https://www.edge.asic.gov.au/ in the browser and using the copy to file option.

2.2.3 Transport Message Layer

A simple subset of SMTP (Simple Mail Transfer Protocol) as defined in Internet IETF RFC 821 and extended by RFC 1830 is used to manage transfer of messages in both directions. The client initiates the conversation and so assumes the role of SMTP sender. The SMTP commands supported are the minimum required to support reliable half-duplex two way communication with recognisable fixed length header which is able to indicate a following variable-length trailer, and also indicate the length of that trailer. The content of the trailer is defined by higher Data Transfer Layers.

SMTP commands supported are:

Command	Description
BDAT nnn	The nnn indicates the number of bytes following the CRLF.
BDAT nnn LAST	The nnn indicates the number of bytes following the CRLF. The LAST indicates end of SMTP message.

2.2.4 Application Session Message Layer

2.2.4.1 Overview

This layer consists of the messages contained in the chunk of data following the BDAT command. There are a number of possible messages in each direction, as defined in the tables below.

The protocol at this level is of necessity state-based - the conversation must be in a specified state for a given message to be valid. If messages are sent to the server in the wrong state, an error message is sent to the client and the connection closed. The client is expected to behave in the same way.

2.2.4.2 Message Content

Messages in this layer contain:

- application layer messages, including digital signatures where required.

Messages are summarised in the tables in the following two sessions, and rigorously defined in the section below titled "Message Definitions".

2.2.4.1 Client Message Summary

Msg id	Description
LOGN	Login message containing userid and password of Registered Agent who is incurring the cost.
BCHN	Inbound batch of EDGE documents including TXID control file.
REQL	Ask the server to send a list of report files previously sent to client which are available for retrieval.
REQO	Request any outstanding EDGE DIS reports waiting for collection
REQP	Request one or more previously sent reports from set of last 3.
PSWD	Password change request
LOUT	Logout - connection then closed.
CLER	Error detected - send message then close connection

2.2.4.2 Server Message Summary

Msg id	Description
LOGR	Login response indicating success or failure of login request
BOUT	Obtain waiting reports from DIS and send BOUT to client
PWCH	Response to password change
SVER	Error detected - send message and close connection.

2.2.5 Application Message Layer

At this layer, communication consists of application messages as defined in the EDGE message specifications - see Appendix B.

There is an additional application-level protocol layer which the client process must incorporate in the client at this, i.e. transport, level so that processing of individual inbound batches of EDGE messages can be tracked reliably. This additional protocol layer consists of requirements for client checks for EDGE DIS Report files. These rules are described in detail below in the section titled “Application-Level Control”.

3. STATE TRANSITION TABLES

3.1 Overview

This section describes processing requirements in the form of state tables. Connections are initiated by clients and once connected a client must send a LOGN message. Thereafter processing is controlled by the server, and the client must, after every message sent, place themselves in the state indicated.

The nature of the DIS system requires the EDGE Internet client to check for waiting reports every time it completes a state-based transaction such as changing the password, sending a batch of documents etc. This is necessary so that the DIS will be in the correct state for the next message.

3.2 Client States

3.2.1 State 1 - Connect

Event id	Event description	Client action	Next state
1	Login	send LOGN message and wait for LOGR reply message	1
2	Receive invalid LOGR	send CLER message with error C01 and close connection	0
3	password ok, no reports waiting	go to next state	2
4	password ok, reports waiting	send REQO message and go to next state	3
5	password expired	send PSWD message to change password	5
6	Receive SVER error message (includes invalid password)	close connection and log error.	0
7	Timeout waiting for server reply	send CLER message with error C02 and close connection	0

NOTES

1. Events 6 and 7 apply to all states.

3.2.2 State 2 - Send Command State Message

Event id	Event description	Client action	Next state
8	Send batch of documents	send BCHN	3
9	Requests list of previous reports	send REQL	4.1
10	Request waiting reports	send REQO	3
11	Password change	send PSWD	5
12	Logout	send LOUT message and close connection	0

NOTES

1. "Command State" is the server state in which it is ready to accept any command which does not have any precursor states.

2. If a BCHN message is sent, then the client system must expect to receive a transmission report for that BCHN in a BOUT message in state 3. If the transmission report is not received but the EDGE Internet server does not indicate an error condition, then this is an error state, and the client system cannot send any more BCHN messages until the discrepancy has been resolved. See the section titled "Application-Level Control" below for more detail.

3. The above note regarding the requirement to receive a transmission report in the next BOUT implies a state which must be persistent across sessions. See the section titled "Application-Level Control" below for more detail.

3.2.3 State 3 - Receive Reports

In this state the client receives all types of outstanding new reports found on the DIS system.

Event id	Event description	Client action	Next state
13	Receive BOUT with 1 or more reports	send REQO to request more reports	3
14	Receive BOUT with 0 reports	go to next state.	2
15	Receive invalid BOUT	send CLER message with error code C01 then disconnect	0

NOTES

1. See the notes for client state 2 above regarding the relationship between BCHN and subsequent BOUT messages containing a DIS transmission report.

3.2.4 State 4 - Request Old Reports

3.2.4.1 Overview

"Old reports" are defined to be report files previously sent by the DIS to the client, whether via the EDGE Internet server or not, that are still available for retrieval via the DIS "Select Old Reports" and"Receive Old Reports" functions. The DIS retains the last 3 of each type of outbound report file for retrieval in this way.

The nature of the DIS protocol as used by the EDGE Internet server makes it necessary to define a new transaction for the process of requesting old reports. This transaction is defined in terms of sub-states to state 4. The transaction consists of:

- it starts with the client sending a REQL message - see state 2 above.

- the server obtains a list of reports from the DIS and sends it to the client as a BOUT message containing each report line as defined by the DIS specifications (see Appendices) with the control data stripped off and LF appended. This means the first 6 bytes (Ctl-B + indicator) are removed, the last 2 bytes (checksum + CR) are removed and CRLF appended. An LF has been included for readability on MS-DOS systems.

3.2.4.2 Sub-state 4.1 - Request Old Reports

Event id	Event description	Client action	Next state
16	Receive BOUT old reports list, user makes no selection	send REQP message with no reports selected, i.e. blank list of report sequence numbers.	3
17	Receive BOUT old reports list, user makes selection	send REQP message to request selected reports	4.2
18	Receive invalid BOUT	send CLER message with error code C01 then disconnect	0

NOTES

1. DIS old report file strings (DIS string type 6) are converted to BOUT report lines as follows:

   - the first 6 bytes (Ctl-B + indicator) are removed.

   - the last 2 bytes (checksum + CR) are removed

   - CRLF is appended. A CR has been included for readability on MS-DOS systems.

2. BOUT report lines after conversion from DIS strings contain up to 3 filenames per line, with each filename prefixed by a sequence number. This sequence number is the number that must be extracted and returned in a REQP message if the client wishes to retrieve the report file named.

3. The client may request more than one file at a time - see the REQP message definition.

4. If event 16 occurs and the client follows the protocol and sends a REQP with no file selection, this will result in the server returning to command state, checking for waiting reports, and sending a BOUT to the client. Hence if the resulting BOUT contains a report, this will be a new report, not an old one. In other words, the client must change state to state 3 after sending the REQP with no file selection, as shown in the table.

3.2.4.3 Sub-state 4.2 - Receive Old Reports BOUT Message

In this sub-state the client receives a BOUT message containing all the old reports requested in state 4.1 above.

Event id	Event description	Client action	Next state
19	Receive BOUT with 1 or more old reports	send REQO to request waiting reports and go to next state	3
20	Obsolete		
21	Receive invalid BOUT	send CLER message with error code C01 then disconnect	0

3.2.5 State 5 - Change Password

Event id	Event description	Client action	Next state
22	Receive PWCH, password changed ok	update system	2
23	Receive PWCH with DIS error, invalid password	advise user to correct and retry at next login	0
24	Receive invalid PWCH	send CLER message with error code C01 then disconnect	0

3.3 Server States

3.3.1 State 1 - New connection

Event id	Event description	Server action	Next client state
1	Message not a valid LOGN	send SVER message with error E03 and close connection	0
2	password ok, no reports waiting	send LOGR message with next state=2	2
3	password ok, reports waiting	send LOGR message with next state=3	3
4	password expired	send LOGR message with next state=5	5
5	DIS error (includes invalid password)	send SVER message with error code set to DIS error and next state 0	0
6	Unable to connect to DIS	send SVER message with error E01	0
7	Timeout waiting for DIS reply	send SVER message with error E05	0

NOTES

1. Events 4 and 6 apply to all states.

2. Timeouts for DIS will be set at 1 minute - if no reply is received from the DIS during that period then something is wrong, so there is not much point waiting.

3.3.2 State 2 - Receive Command State message from client

Messages received in this state are those which are stateless in the sense that there are no pre-requisite messages. For example, an REQP requires a previous REQL message, so an REQP cannot be sent without warning, and so is state-dependent. On the other hand a BCHN message does not have any precursor messages and so is regarded as stateless.

Event	Server action	Next client state
Receive BCHN message	Send BCHN file to DIS, collect next waiting report (should be transmission report) and send to client as a BOUT message.	3
Receive REQL message	Send requests to DIS to retrieve list of old files until end-of-list message received from DIS, then send reply as a BOUT message.	4
Receive REQO message	Send request to DIS to retrieve next waiting report and send to client as a BOUT message. If client receives a report then they stay in state 3 and send another REQO, otherwise they go to state 2, command state.	2 or 3
Receive PSWD message	Send a password change request to the DIS	5
Receive LOUT message	Send a logout message to the DIS and close connection	0
Receive CLER	Send a logout message to the DIS and close connection	0

NOTES

1. "Command State" is the server state in which it is ready to accept any command which does not have any precursor states. It could also be regarded as a "main menu" state.

2. Events in this state are always user-initiated.

4. MESSAGE DEFINITIONS

4.1 BCHN - Batch from Client

This message contains an EDGE transmission.

Seq	Count	Object	Description
1	1	Message header	BCHN header - see below
2	1	EDGE message	An EDGE transmission consisting of 1..99 EDGE documents and a TXID control file, as defined in EDGE message specs.

BCHN Message Header

Seq	Type	Length	Description
1	A	8	Message id - literal 'XSCBCHN' + LF character (hex 0A)
2	A	13	User defined reference "File" name in DOS standard 8.3 + LF char (hex 0A0) for the document which follows. This is used in the Transmission report to identify the file.

NOTES

1. No delimiter is necessary between messages because the message header, trailer and signature segments can be used to identify start and end of messages.

2. Fixed length fields in this and all messages are to be padded with trailing space characters for alpha fields, or leading '0' characters for numeric fields.

4.2 BOUT - Batch of Outbound Reports

This message consists of a set of one or more text report files waiting to be sent to the agent. Files are simply concatenated, preceded by a separator which includes the filename. At present only one file is sent at a time, but the message structure allows for more than one.

Seq	Count	Object	Description
1	1	Message header	BOUT header - see below
2	1..n	EDGE reports	EDGE report files, preceded by BOUT separator - see below

BOUT Message Header

Seq	Type	Length	Description
1	A	8	Message id - literal 'XSVBOUT' + LF character (hex 0A)
2	N	3	Count of files which follow

BOUT Separator

This separator is used to precede report files in the output message.

Seq	Type	Length	Description
1	A	10	Literal 'XSVSEPRXXX'
2	A	13	Filename of file which follows, in DIS standard 8.3 + LF char (hex 0A)

Note that the DIS supplies files one at a time so that there can only be one file lost if there is a communication failure. The EIS will only retrieve this one file, hence the BOUT will only contain one file. Clients cannot be sure that they have retrieved everything until they receive a BOUT message indicating no waiting output. Clients must therefore use the REQO message until they receive a BOUT message with a file count of zero before they can move on.

This message is also used to send a list of files previously sent by the DIS to the client and still available for retrieval. This is sent in response to a previous REQL message. The list is sent in the form of a single report consisting of 1 or more text lines delimited by a CRLF. The format of each line is as defined in the DIS spec.

This message is also used to send one or more previously-sent files included in a prior REQL list and requested by a REQP message. When used in this way, the message may contain more than one file.

4.3 CLER - Client Error

This message is for use when the client system encounters an error and wishes to advise the server that it cannot continue processing and must terminate the session.

Seq	Type	Length	Description
1	A	8	Message id - literal 'XSCCLER' + LF character (hex 0A)
2	A?	3	Error code
3	A	0..512	Variable length descriptive information - free format text

This message is provided primarily to assist in fault investigation. Its use is entirely optional.

4.4 LOGN - Client Login

This is the first message that the client sends and is sent immediately after the client establishes a TCP connection with the server. Hence when the server receives a connection request it opens the connection and expects to immediately receive this message.

Seq	Type	Length	Description
1	A	8	Message id - literal 'XSCLOGN' + LF character (hex 0A)

2	A	6	EDGE DIS userid
3	A	16	EDGE DIS password

4.5 LOGR - Server Response to Login Request

This message is sent by the server in reply to the client login request. It contains the result of login request processing - either the request is accepted, meaning the client can proceed to send a message, or the request is rejected, in which case the message contains rejection reasons.

The message includes the name of the last file that the DIS sent to the client. This should be used by the client system to ensure that it detects non-receipt of a report file. More details on this are provided in the section below titled "Application-Level Control".

Seq	Type	Length	Description
1	A	8	Message id - literal 'XSVLOGR' + LF character (hex 0A)
2	A	3	Result code - '000' if login accepted, else rejection error code - see below,
3	N	1	Next client state required. Can be: • 0=disconnect • 2=send command state message • 3=receive reports • 5=change password
4	A	12	Name of the last file that was sent by the DIS system

Error Codes

Code	Description
Dnn	DIS error codes - see DIS comms spec

4.6 LOUT - Client Logout

This is sent by the client when it wishes to advise the server that it has completed it's session and is about the close the connection.

Seq	Type	Length	Description
1	A	8	Message id - literal 'XSCLOUT' + LF character (hex 0A)

The client must close the connection immediately after sending the message.

4.7 PSWD - Client Password Change Request

This message is used by the client to request a change to the DIS password. The message contains the new and old passwords, which must conform to password rules as defined in the EDGE Message Specification.

Seq	Type	Length	Description

1	A	8	Message id - literal 'XSCPSWD' + LF character (hex 0A)
2	A	16	Existing EDGE DIS password
3	A	16	New EDGE DIS password

4.8 PWCH - Server Response to Password Change

This message is sent by the server in response to a password change request.

Seq	Type	Length	Description
1	A	8	Message id - literal 'XSVPWCH' + LF character (hex 0A)
2	A	3	Result code - '000' if password changed ok, else EDGE DIS rejection error code

4.9 REQL - Request List of Old Reports

This message is used by the client to request a list of files previously received from the DIS which are still available for retrieval.

Seq	Type	Length	Description
1	A	8	Message id - literal 'XSCREQL' + LF character (hex 0A)

4.10 REQO - Client Request DIS Output

This message is used by the client to ask the server to check if there is any DIS output, and return any waiting files.

Seq	Type	Length	Description
1	A	8	Message id - literal 'XSCREQO' + LF character (hex 0A)

The server will return either waiting output or a BOUT message with a file count of zero to indicate no output.

4.11 REQP - Client Request Previous DIS Report

This message is used by the client to ask the server to use the DIS facility for retrieving reports from the last 3 of each type saved in the EDGE DIS mailbox for the client. This allows the client a limited facility for retrieving a report they have previously retrieved but have lost. If the desired report is not in the last 3 the clients will have to contact ASIC support staff to request manual retrieval of the required report. Refer to the EDGE DIS specifications for further information - see the Appendices.

Seq	Type	Length	Description
1	A	8	Message id - literal 'XSCREQP' + LF character (hex 0A)
2	A	32	Comma separated list of report sequence numbers

NOTES

1. The server will retrieve the list of previously sent reports available for retrieval and return the list as a BOUT message containing the list of filenames returned by the DIS. The exact format of this list is described in section "3.2.4 State 4 - Request Old Reports". This list is essentially a list of filenames preceded by sequence numbers. For further information refer to the DIS specifications - see the Appendices.

   The client system must make a selection of one or more files from the list, possibly with user input, and send this set of selections to the server in a REQP message in the form of a comma-separated list of sequence numbers identifying the desired filenames. The list must have no embedded spaces. The list can contain any number of selections up to the limit of the fixed field length.

   The server will then request the set of files from the DIS and return it as a BOUT message.

4.12 SVER - Server Error Message

This message is used by the server to advise the client of an error condition. Error conditions will be DIS errors, loss of connectivity with the DIS, or any other condition where the server cannot continue the conversation.

Seq	Type	Length	Description
1	A	8	Message id - literal 'XSVSVER' + LF character (hex 0A)
2	A	3	Error code - either Dnn EDGE DIS error, or Enn error from table below.
3	A	0..512	Variable length descriptive text - free format text

Error Codes

Code	Description
E01	Lost connection to DIS
E02	Misc error - unable to continue processing
E03	Protocol violation
E04	Previous message had incorrect format
E05	Timeout waiting for reply from DIS

5. APPLICATION-LEVEL CONTROL

5.1 Overview

As mentioned above, there are additional client application-level requirements which cannot be easily incorporated into the application session-level protocol described above, because the processing takes place at a higher level. Adherence to these requirements will ensure that a client system can reliably recover from any problems caused by EIS communication failures.

5.2 Client System Requirements

5.2.1 Ensure All Missing DIS Report Files Retrieved

Client systems must reliably identify missing files. The login reply message, LOGR, informs the client system of the last report file that the DIS system sent. The client system is required at the time of LOGR receipt to verify that the file named in the message has in fact been received. If the file has not been received, then the client system is required to ensure that the missing file is retrieved. This can be done using the messages described above as follows:

- use the REQL messages to request a list of previously sent reports available in the DIS for retrieval by the client.
- examine the list and locate the missing file, if present.
- use the REQP message to request the missing file be resent.

If the missing file is not included in the list of previously sent reports, or if the system is otherwise unable to retrieve the missing file, then the client system operator must be informed of this. Operating procedures must require the client operator to contact ASIC via standard EDGE customer support channels to request recreation of the missing report file.

Note that this is the same requirement as exists with the DIS system. It is very rarely required. The point is that client systems must be capable of handling the situation.

Note – for PDF outputs by ASIC, the ISO-8859-1 character set is used.

5.2.2 Ensure All DIS Transmissions Accounted For

In addition to ensuring that all missing files are accounted for, client systems must ensure that they either receive a DIS transmission report for every BCHN sent, or they verify by checking the last filename sent field in the LOGR message that the BCHN in question was not received. This is a requirement imposed by the DIS system: since the DIS Transmission Report acts as a transmission receipt, client systems must ensure they obtain it before continuing. Developers are referred to the DIS documentation described in the appendices.

5.3 Failover

5.3.1 Failover Facilities

Failover is possible in the event of loss of two ASIC network components:

- loss of EIS connectivity - in this case the client cannot connect to the EIS.
- loss of EDGE mailbox processing - if this occurs the client will be able to connect to the EIS, but may be unable to lodge documents or receive reports. Reports may also be delayed.

If either of these events occur then it is possible to continue processing new documents by connecting to the alternate EIS host, and hence also the alternate EDGE mailbox.

5.3.2 Failover Not Automated

Failover in these situations cannot be automated and has to be left to the client because of the preservation of state between the client system and the EDGE mailbox which the EIS lodges documents into. In other words, if an EIS host cannot be contacted, then the client must decide if they want to suspend processing or switch to the alternate EIS host and hence EDGE mailbox.

5.3.3 What Client Must Be Aware Of

If the client decides to switch to the alternate host, then they must be aware of the following:

- the LOGR message field showing the name of the last file sent by the DIS will probably not be the last file received by the client system.
- EDGE DIS transmission numbers will probably not continue in sequence from before the switch.
- EDGE report filenames will change. The primary mailbox generates filenames (transmission, validation, outbound, etc) which end with the string “_PR.”, whereas the secondary mailbox uses “_SE.” instead.

5.3.4 Recovery From Orphaned Transmissions

An “orphaned” transmission is here taken to means a transmission lodged with ASIC for which all expected reports have not been received due to loss of an essential part of the ASIC eBusiness network. In this situation, the client has two choices to complete processing of the affected transmissions:

- wait until ASIC returns to normal service
- switch to the alternate EIS host and attempt recovery

In fact complete recovery is not possible until the original EIS host and corresponding EDGE mailbox return to normal service. However in many cases the client can effectively recover:

- if the outstanding document is a 201, enquire on the company name via ASIC Netsearch at http://www.asic.gov.au. If the company has been incorporated, then request a reprint of the Certificate of Incorporation.
- if the outstanding document is a 410, enquire via Netsearch as above. If the name is reserved, the reservation worked.

Note that the main thing to focus on here is the fact that failover provides a facility hitherto missing: If the ECR service is unavailable, it will generally be possible to continue with new work by switching to the alternate EIS.

6. ERROR HANDLING

6.1 Overview

The general approach taken to error handling is to log the error and attempt to return an error message to the client. The server will then close the connection.

6.2 Timeouts

A general timeout limit of 1 minute is applied to client sessions, hence the server expects to receive a reply from the client within 1 minute of having last sent a message to the client.

Clients are expected to do the same, thus if the client does not receive a message from the server within 1 minute then it should simply abandon the session and close the connection.

Appendix A - Amendment History

Version 0.80

31/03/1998 - First draft version published for comment.

Version 0.90

30/06/1998
First draft corresponding to working test system. Minor adjustments to messages. “Application-Level Control” section re-written.

Version 0.95

04/09/1998
This release contains only changes notified by ECR_Change_1.doc issued on 15th July, 1998.

Corrections to next states:

1. p6, section 3.2.1, event id 6, next state is 0
2. p9, section 3.2.4.3, event id 20, change Client action from “Send CLER message...” to “goto command state”.
3. p9, section 3.2.5, event id 23, add to Client action “ to correct and retry at next login”., change Next state from 23 to 0.
4. p9, section 3.3.1, change “Next state” column header to “Next client state”. Event id 3, set Next client state to 3. Event id 4, change Server action from “...next state=4” to “...next state=5”, also change Next client state from 4 to 5.
5. p10, section 3.3.2, change “Next state” column header to “Next client state”.
6. p12. section 4.5, item seq 3, Description of possible next client states should read “0=disconnect, 2=send command state message, 3=receive reports, 5=change password.”

Version 1.00

09/10/1998
First production release. This contains no changes except to remove the draft status and update the version number.

Version 1.01

18/01/1999
Section 2.2.2. Add second paragraph warning that client packages must operate SSL securely.
Section 3.2.4.2 Change event 16 to send a REQP requesting 0 old reports. Add to client action of event 16: “send REQP message with no reports selected, i.e. blank list of report sequence numbers.”
Add note 4: “If event 16 occurs and the client follows the protocol and sends a REQP with no file selection, this will result in the server returning to command state, checking for waiting reports, and sending a BOUT to the client. Hence if the resulting BOUT contains a report, this will be a new report, not an old one. In other words, the client must change state to

state 3 after sending the REQP with no file selection, as shown in the table."
Section 3.2.4.3 Change event 19 to send a REQO to check for waiting reports.
Mark event 20 obsolete. This situation never occurs.
Section 3.3.2. Minor corrections to server state stable:
1. Change wording of BCHN message - only gets one report at a time.
2. Add REQO message, which is valid in this state.

Version 1.02

20/07/2000
Section 2.2.1. EIS failover description added. Client software should use hostname and DNS, and not hardcode IP addresses.
Section 5.3 Failover added/

Version 1.03

14/08/2003
Section 2.2.2
1. Correct typo joining last sentence of 2.2.1 to title of 2.2.2
2. Add description of publication of CA certificate of the CA who issued the EIS server certificate.

Misc – correct page header version number.

17/05/2012
Section 3.2.2
State 2 – Send Command State Message
Amend Note 2

12/01/ 2015
Section 2.2.2 Security Layer
Remove URL reference

27/01/2016
Section 4
Correct sequence number errors in the BOUT separator, LOGN and SVER messages
Section 5.2.1
Add reference to character set used on PDF outputs.