THE STOCK EXCHANGE OF HONG KONG LIMITED

ISSUER INFORMATION *feed* SERVICE
(NEWS HEADLINE)
("IIS News Headline")

Transmission Specification

Version no.: 1.4

Date: 19 Dec 2012

Modification History

Version	Date	Description and reason for modification
1.0	23 May 2011	This is the first draft for internal comments
1.1	18 Nov 2011	1. Add Tier 2 code 15000, 12951, 12952, 12953, 12954, 12955, 12956, 12957, 23500
1.2	9 Feb 2012	1. Add Tier 1 code 55000
1.3	30 Nov 2012	1. Add Tier 2 code 17960, 19750 2. Amend Tier 2 code 19550
1.4	19 Dec 2012	1. Add Tier 2 code 12958 & 40400 2. Amend Tier 1 code 40000 3. Amend Tier 2 code 17100, 17150, 25100 & 25200

TABLE OF CONTENT

1. Introduction

1.1. Overview

Issuer Information *feed* Service (IIS) is a system of the Stock Exchange of Hong Kong Limited ("the Exchange") which distributes issuer information that includes Listed Company news, Exchange news and issuer documents. The Exchange offers two datafeed products under the IIS system, namely, IIS which covers both news headings and contents; and IIS (News Headline) which provides only the news headings. This document provides message definition and application protocol between IIS and IIS subscribers /distributors/ information vendors (hereunder collectively abbreviated as "Vendor") who subscribe for IIS (News Headline). It also describes the error handling and recovery procedure.

The intended reader of this document is the technical personnel of a company that has subscribed for IIS (News Headline). The technical personnel should acquire basic knowledge of cryptographic technology and XML (Extensible Markup Language). This specification provides sufficient information for Information Vendors to develop their own systems to receive issuer information from IIS.

Readers please note that the term "IIS" in the later text in this document refers to the IIS system which delivers the IIS (News Headline) service.

1.2 Document Structure

Section 2	*System Overview* This section describes the scope, constraints and application protocol of IIS.
Section 3	*Line Protocol* This section describes the communication means between IIS and system of the Vendor
Section 4	*Detailed Message Format* This section describes the message format in details
Section 5	*Detailed Message Processing and Application Protocol* This section describes the message processing and application protocol in details
Appendix	This section contains several subsections for detailed implementation. It includes: *XML schema* *Base64 encoding and decoding algorithms* *Cryptography in IIS* *An example of Message Flow Diagram* *Error Code Definition* *Subject Code within DescriptiveMetaData* *MIME Type – File Extension Mapping*

1.3 Document Convention

[data format] variable to be substituted which compiles with data format

data format includes : X – character
9 – [0-9] numeric value
N – [0-9] character included leading zeros.
* -- zero or more
+ -- one or more

For example:

[X]* refer to a string including empty string: "123", "test"
[X]+ refer to a string with at least 1 character.
[9]*3 refer to a numeric value 0-999
[N]*5 refer to a numeric string 0000 - 99999

2. System Overview

2.1 Scope

IIS (News Headline) provides headings of real time news to Information Vendors and this covers the following categories.

1. Exchange news
2. Listed Company news
   - Main
   - GEM

All the news collected for distribution in IIS (News Headline) is generally named as news in the subsequent sections of this document.

2.2. IIS Operation Hours

IIS operates during Securities Market trading days from Monday to Friday and day immediately before the first trading day of any given calendar week. Specifically, IIS operation hours are as follows:

2.2.1 Trading Days

a) System Hours:
- Ready for Logon at 05:30
- System Shut Down at 00:00 (next day)

IIS (News Headline) would provide one day online news headings to Vendors. After IIS System is restarted in the morning, only current day's news will be available (i.e. from 0:00 onwards)

b) Business Hours (with news / document distribution):
- Mon - Fri 06:00 - 23:00

2.2.2 Day (including mid-week public holiday) immediately before the first trading day of any given calendar week

a) System Hours:
- Ready for Logon at 17:30
- System Shut Down at 21:00

IIS (News Headline) would provide one day online news headings to Vendors. After IIS System is restarted in the morning, only current day's news will be available (i.e. from 0:00 onwards)

b) Business Hours (with news / document distribution):
- 18:00 – 20:00

All non-IIS operation hours, i.e. any time outside a) and b) in 2.2.1 & 2.2.2 above, will be reserved for maintenance.

An Illustration for April 2006:

Sun	Mon	Tue	Wed	Thu	Fri	Sat
						1
2 B	3 A	4 A	Ching Ming Festival 5 B	6 A	7 A	8
9 B	10 A	11 A	12 A	13 A	Good Friday 14	15
16	Easter Monday 17 B	18 A	19 A	20 A	21 A	22
23 B	24 A	25 A	26 A	27 A	28 A	29
30	Labour Day 1 B	2 A				

Note:
Saturdays, Sundays and holidays are shaded in grey.
IIS will be brought up on Days marked with "A" and "B" which represents:
A days – follow the schedule stated in section 2.2.1, being Trading days
B days – follow the schedule stated in section 2.2.2, being Day (including mid-week public holiday) immediately before the first trading day of any given calendar week.

2.3 Information Delivery

Once the Vendor has logon to IIS, updated and subscribed headline is delivered to the Vendor automatically. Each headline contains unique headline identity, news information, e.g. category, date/time in ISO 8601 format, language in ISO language code (ISO639-ISO3166).

The headline is in XML format while they are devised with reference to NewsML Version 1.0 of International Press Telecommunication Council. The functional specification of NewsML Version 1.0 was updated on 24th October 2001. It is available in public Internet, http://www.iptc.org. The specification can be found with this URL http://www.iptc.org/site/NewsML/specification/NewsMLv1.0.pdf.

Additional XML tags are defined to enclose headline, control flow, command and status response instructions and the final XML form is called message block. These message blocks are transferred over TCP/IP session that has been established between IIS and Vendor's terminal.

More detailed descriptions on the messaging interface are given in the following sections.

The message block is classified into three types, command/response, data and control flow. It takes the following form.

```
<?xml version="1.0"?>
<NDSML>
   <MsgHeader>
      <MsgDate>.....</MsgDate>
      <MsgID>.....</MsgID>
      <MsgType>.....</MsgType>
  </MsgHeader>
  <[MsgID]>
      .....
  </[MsgID]>
</NDSML>
```

Tag	Format	M/O	Occurs	Description
NDSML	Complex	M	1	IIS Message root tag

MsgHeader	Complex	M	1	Message header information
MsgDate	CCYYMMDDT24HHMISS[+-]NNNN	M	1	Message delivery date time
MsgID	[X]*20	M	1	Message code/Command
MsgType	[NDScmd/NDSdata/NDSctrl]	M	1	Message Category code
[MsgID]	[X]*	M	1	Message ID

The following table summarises the types of message used in IIS.

Message category	**Message type**	**Message_code**
Command/response	NDScmd	INITREQ INITRESP LOGONREQ LOGONRESP LOGOFF CHNGPWDREQ CHNGPWDRESP FULLRECVYREQ PARTRECVYREQ RECVYRESP RECVYCOMPLETE PERMISSIONDROP
Data	NDSdata	UPDATEHEADLINE RECVYHEADLINE
Control flow	NDSctrl	STATUSREQ STATUSRESP

2.4 Application Protocol

The Application protocol covers the following areas.

- Logon and Logoff
- Normal transmission
- Error recovery
- Message handshake

The first three items fall into command/response and data categories while the last one belongs to control flow category.

The following provides an overview to the protocol used in the application. Please refer to the detailed message processing and application protocol section for a detailed description of each kind of application messages.

2.4.1 Logon and Logoff

Having established the TCP/IP connection with IIS, the Vendor sends INITREQ command to IIS. IIS responds with INITRESP response together with logon information and session key encrypted by IIS symmetric key using Triple-DES algorithm (see Appendix C for details). The Vendor makes LOGONREQ command with Vendor identity and password encrypted by the session key using Triple-DES algorithm. Having verified the Vendor information, IIS gives back LOGONRESP response together with logon response information. It should be noted that each Vendor identity can only be used for one connection with IIS while duplicate logon is guarded in IIS. Once duplicate logon from same Vendor (Determined by connection using same Vendor identity) is detected by IIS, all connections using the same Vendor identity will be dropped. If the Vendor fails to logon to IIS for 9 times (subject to change by the Exchange), its account is de-activated. The Vendor must contact the Exchange or its dedicated agent in order to access the service again.

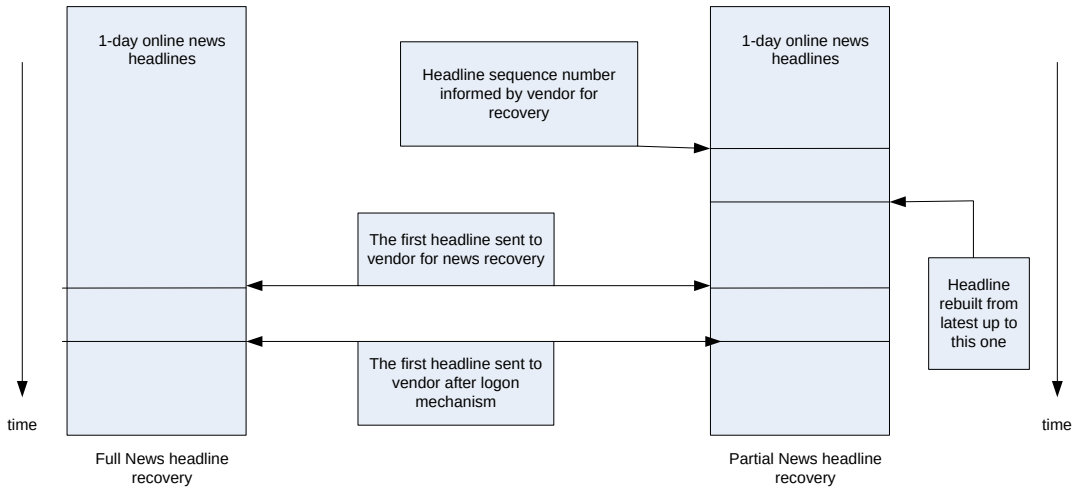
When the Vendor would like to stop receiving updated news, the Vendor can issue a LOGOFF command to inform IIS. However, if the Vendor would like to receive updated news again, the Vendor must issue INITREQ and then LOGONREQ commands again. If the Vendor system is closed without sending LOGOFF command, IIS will discover the disconnection based on the message handshake protocol or TCP/IP layer whichever comes first.

2.4.2 Normal Transmission

After the Vendor terminal has gone through logon process, subscribed headline just received from IIS is delivered to it using unsolicited data response. Each headline sent from IIS no matter which subtype it belongs to (to be described in later section) is assigned a sequence number and this sequence number “Headline Sequence Number” is used for partial headline recovery. However, this sequence number may not be in consecutive sequence depending on what kinds of news the Vendor has subscribed.

2.4.3 Error Recovery

The Vendor can initiate a recovery request to recover up to 1 day's online news headlines from IIS. Two levels of recovery are provided for the Vendor. Firstly, a recovery of 1 day's online headline request can be made. The recovered headline is sent to the Vendor terminal in a last-in-first-out order. Secondly, partial online headline recovery can be requested. The Vendor needs to inform IIS the last news it kept within its own system (identified by the sequence number of headline) and IIS will rebuild the successive headlines also in last-in-first-out order. It should be noted that the most recent news received from IIS is also sent to the Vendor at the same time. The following diagram depicts the news recovery mechanism.



For full recovery, the Vendor should send FULLRECVYREQ command to IIS. IIS will accept FULLRECVYREQ only right after the logon request completed successfully. IIS will ignore any FULLRECVYREQ once news has been dissemination after Vendor logon. This feature is designed to avoid unnecessary full recovery requests made by vendors which may affect their system performance. For partial recovery, the Vendor should send PARTRECVYREQ command with last "Headline Sequence Number" to IIS. In both cases, IIS will respond with RECVYRESP with the total number of recovery headlines to be sent to the Vendor. Then, IIS will rebuild the recovery headline for the Vendor using unsolicited data response RECVYHEADLINE. After all recovered headlines are sent, IIS sends status response RECVYCOMPLETE to the Vendor.

Due to the long lead time required for full news recovery during the operation hours, direct connection IIS vendors can only request one full news recovery through a single connection session. A re-connection is required for additional full news recovery. Vendors are advised to perform full news recovery on one of the dual live connections, but not both at the same time.

2.4.4 Message Handshake

Status request feature is available to improve the communication fault detection time. Thus, when no traffic is detected from the Vendor terminal for 120 seconds (subject to change by the Exchange), IIS sends STATUSREQ command to the Vendor terminal and expects Vendor to respond with STATUSRESP. If the Vendor terminal does not respond to the status request for 120 seconds, IIS would issue STATUSREQ command again. If IIS does not get any response, it would disconnect the established connection with that Vendor terminal. Vendor can also issue this status request to detect if IIS is still running when there is no traffic from IIS for 60 seconds.

2.5 IIS Certification Test

Vendors who choose direct connection with IIS system have to pass the IIS (News Headline) Certification Test according to the requirements as set out in the IIS (News Headline) Certification Test Procedures (This document will be provided by Exchange upon IIS (News Headline) service application) before they will be granted the IIS (News Headline) license. The IIS (News Headline) Certification Test will cover all requirements set out in this document. Apart from the IIS (News Headline) Certification Test, direct connection IIS (News Headline) vendors must meet all the requirements as set out in this IIS (News Headline) Transmission Specification.

3. Line Protocol

Item	Description
Mode of transmission	IP-based Network
Communication line speed	2Mbps, 3 Mbps and 4Mbps available*
Communication protocol	TCP/IP (port number 20, 21 for file transfer & 6800 for IIS headline and command messages)
Allocated Bandwidth	- 128Kbps for IIS headline and command messages (For current MDS subscribers, 128Kbps should be allocated for IIS headline and command messages)
TCP Receive Buffer Size	64K Bytes

3.1 IIS Connection Ports in the Primary Site

For each Vendor identity, it is given two sets of IP addresses representing one primary and one secondary connection ports on the IIS Primary production system ("the Connection Ports"). If Vendor found that no TCP/IP connection can be established after 3 times of retry on each IP address, it should stop its system and find out if there is any problem with the physical connections.

Under the standard configuration of single live connection (with one live feed), IIS will provide two production Connection Ports and allow each Vendor to maintain only one logon session using one Vendor identity.

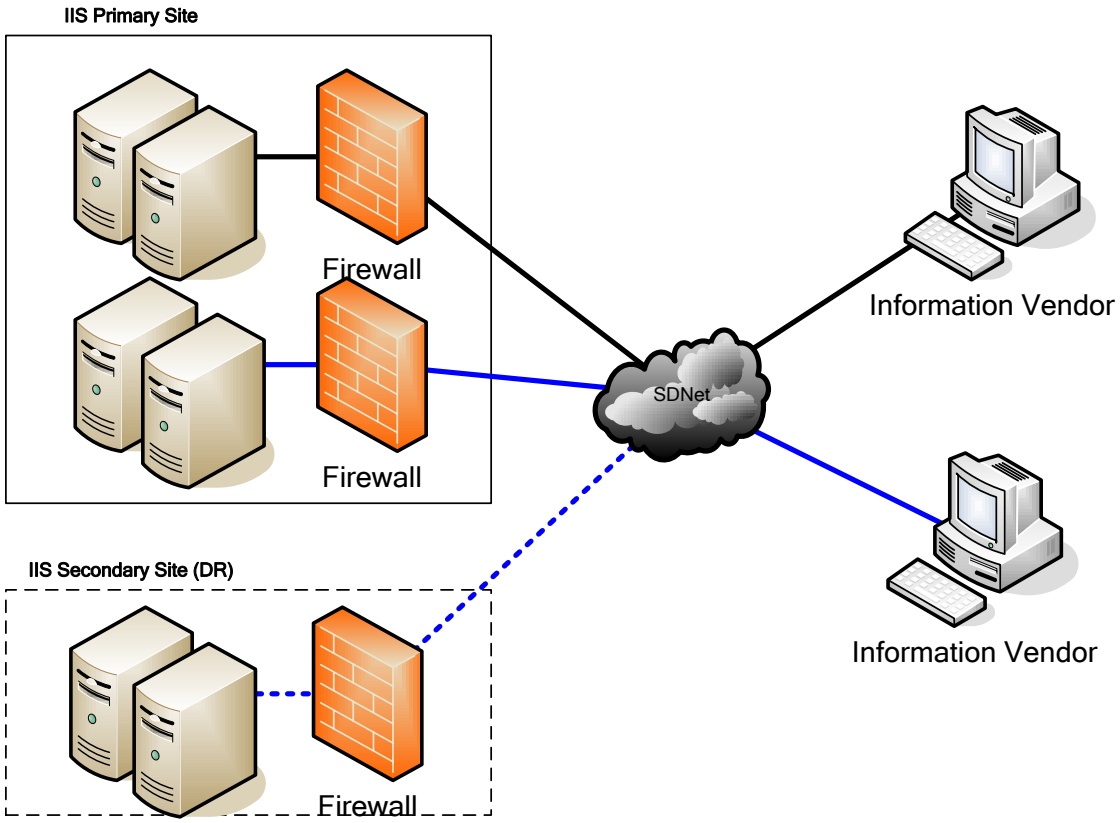
3.2 IIS Disaster Recovery Port in the Secondary Site

In order to increase the availability of IIS, a Secondary Site for IIS is introduced. Each Vendor will be provided with a single Disaster Recovery Port. A Disastery Recovery Port contains an IP address of IIS Data Delivery Server for headlines and command messages.

When site failover is triggered, Vendor will just need to switch their connection from the Primary Connection Port to the Disaster Recovery Port. Instead of using the connection ports for the Primary production system, Vendor had to use the Disaster Recovery Port in the Secondary Site. An additional Disaster Recovery Recovery Port could be arranged but is subject to additional charges.

3.3. Network Diagram

Network Diagram for Live-Live Connection Configuration



3.4 Line Connection Failure

Information Vendor is recommended to detect connection status in the TCP level so that link failures can be identified.

Information Vendors are requested to implement auto-detection of line failure and auto-reconnection of its production line. This would help to shorten blackout time and ensure continuity of news transmission.

3.5 Failure of the IIS System in Primary Site

If IIS system in Primary Site fails, IIS site failover will be triggered. The operation will take approximately 30 minutes to fail IIS over to the Secondary Site and ready for news dissemination. After failover to Secondary Site, IIS would be in a state which is ready to perform full news recovery. Upon receiving notification from the Exchange, Vendor will be required to connect to IIS Secondary Site via the Disaster Recovery Port.

Right after switching from the Primary site to the Secondary Site, Vendors should perform a full recovery to make sure their system will not miss any news that may be published during the failover period.

3.6 Guidance for Vendor during IIS Failover

Pre-requisites for failover to the Secondary Site:

- Disaster Recovery Port in the Secondary Site is ready;

- User ID and password is ready (Any new password change on the failover day will be lost and old password is expected to be used after failover to the Secondary Site);
- Information vendors should perform their housekeeping wherever applicable. i.e. to record the headlines or attachments which have yet been completely received before failover.

Steps for reconnecting to the Secondary Site of IIS:

- Attempt the Disaster Recovery Port in Secondary Site;
- Issue logon request and complete the logon process as usual;
- Issue full recovery request;
- Start receiving full set of news headlines (reverse chronological order with latest news transmitted first) for current day. Vendor should note that the following special handling is required:
  - The sequence number for news after site failover will start from 1. It also applies to failover from the Secondary to Primary Site as well;
  - The Vendor's software should check if there are duplication of headlines received. It can be done by checking the Headline <ProviderID>, <DateID> and <NewsItemId> (refer to section 5.2.1 for details).

4. Detailed Message Processing and Application Protocol

There are three kinds of message category, command/response, data and control flow. The command instructions are sent from the Vendor to request services of IIS, such as request for connection and data recovery. Data message category is focused on headline delivery which is delivered in an unsolicited way. The third type, control flow, is an interactive way of communication. IIS can detect if the Vendor system is up and running and vice versa.

4.1 Command/Response Messages

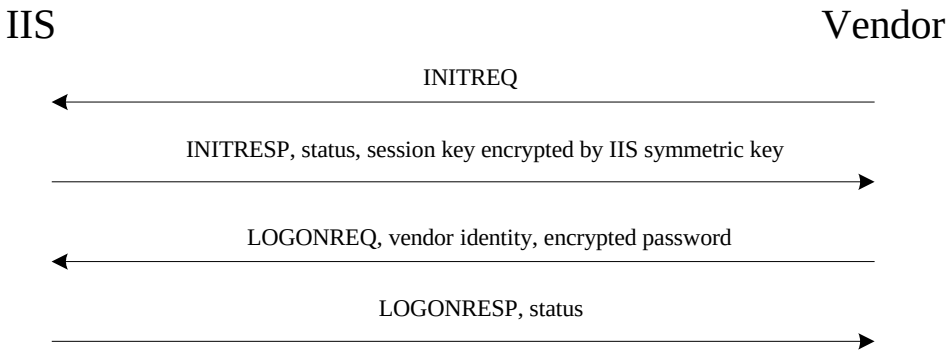
These messages are used for connection request and data recovery. The "MsgID" is among one of the following values.

Message code	Message originator	Description
INITREQ	Vendor	Request to communicate with IIS
INITRESP	IIS	Asking the Vendor to send Vendor identity and encrypted password
LOGONREQ	Vendor	Sending Vendor identity and encrypted password for authentication
LOGONRESP	IIS	Responding if the service is granted or denied to the Vendor
LOGOFF	Vendor	Disconnecting from the existing service
CHNGPWDREQ	Vendor	Request to change the password
CHNGPWDRESP	IIS	Responding if the change of password instruction is successful
FULLRECVYREQ	Vendor	Full headline recovery
PARTRECVYREQ	Vendor	Partial headline recovery
RECVYRESP	IIS	Headline recovery response
RECVYCOMPLETE	IIS	Notification of the completion of headline recovery
PERMISSIONDROP	IIS	It is a notification to Vendor that the Vendor identity cannot be used to get service from IIS

For the Request/Response messages, there is one "ReqID" attribute at both request/response "MsgID" tag to associate the response message to the request message. Vendor should issue the request command with a unique "ReqID" assigned that IIS will respond with the same "ReqID". This can be achieved by an incremental sequence number.

4.1.1 Logon

There are two steps during logon process as shown after the Vendor establishes TCP/IP connection with IIS. If the connection cannot be established with the primary address, the secondary address should be tried.



Firstly, the Vendor initiates INITREQ request to IIS. IIS responds with INITRESP response message to the Vendor. The following response status is found.

Response status	Additional information/Error Code	Description
SUCCESS	Session key encrypted by IIS symmetric key using Triple-DES algorithm which is described in Appendix C	Successful status with session key for password encryption in next step
FAILURE	INVALID_MESG	Invalid Message Format
FAILURE	SERVICE_NOT_AVAILABLE	Service not available

The session key is used to protect sensitive information, e.g. password, transferred between IIS and Vendor. This key in big-endian format is encrypted by IIS symmetric key using Triple-DES algorithm and then it is transformed to Base64 format. For details, please refer to Appendix C. The IIS symmetric key is distributed to each Vendor. The session key is invalidated after either the Vendor issues LOGOFF command or either one of parties is disconnected.

Secondly, the Vendor sends LOGONREQ request with Vendor identity and encrypted password with session key using Triple-DES algorithm to IIS (please see Appendix C for details). The encrypted password should be transformed to Base64 format before transmission. IIS will respond with LOGONRESP and logon status to indicate whether the service is granted or denied. After successful logon, the Vendor can request other services such as change of password and headline recovery while updated and subscribed headline is delivered to the Vendor automatically. Thus, if the Vendor requests these types of service before the logon process, IIS will respond with failure status code. The following response status for LOGONRESP can be found.

Response status	Additional information/ Error Code	Description
SUCCESS	Kind of services (HDL) Subscribed package (A or B or C)	Successful status indicating what kind of services is granted (headline)
FAILURE	INVALID_MESSAGE	Invalid message format
FAILURE	INCORRECT_SUBSCRIBER	Incorrect Vendor identity or password
FAILURE	PERMISSION_DROP	Operation not allowed because permission is dropped
FAILURE	DUPLICATE_LOGON	A connection has been established for same Vendor identity and password. All connections from the same Vendor Identity will be dropped.
FAILURE	SERVICE_NOT_AVAILABLE	Service not available

If the Vendor fails to log on to IIS for 9 times, the account is de-activated. “PERMISSION_DROP” status response message is returned on 9th time of failure. The Vendor must contact the Exchange or its dedicated agent in order to access the service again.

If response message of “FAILURE” with “DUPLICATE_LOGON” error code is received, the Vendor should initiate connections to IIS again.

The Vendor can choose to initiate a full or partial recovery request after successful logon to IIS in order to ensure there is no outstanding headline pending received. For partial headline recovery, the IIS may respond RECVYRESP with Error code = NEWS_NOT_FOUND. Under this situation, there are no outstanding headlines in IIS and the vendor need to send FULLRECVYREQ command back to IIS for retrieving current day’s outstanding headline.

4.1.2 Logoff

When the Vendor does not want to receive updated headline and to get any kind of service from IIS, the Vendor terminal can issue LOGOFF request to inform IIS about this. However, IIS would still issue STATUSREQ command to find out if the Vendor terminal is running. If the Vendor does not respond this command twice, IIS will drop the connection. When the Vendor would like to communicate with IIS, the Vendor must issue INITREQ and then LOGONREQ commands again. When TCP/IP connection is still

maintained, another Vendor using same Vendor identity and password is not allowed if the Vendor does not issue LOGOFF command. "Duplicated logon" is resulted for that new connection.

Any invalid message format for LOGOFF command will be discarded in IIS. As a result, updated headline is still sent to the Vendor. If the Vendor does not issue LOGOFF command for service disconnection before dropping the TCP/IP connection, IIS will discover the disconnection via the STATUSREQ. It might take about two minutes for IIS to find out if the connection is actually gone, however, this elapse time is only indicative and may vary accordingly depending on different Vendor's setup.

Once IIS acknowledges the successful status of LOGOFF command, the session key created during logon process is invalidated. The Vendor must issue INITREQ again to establish new session.

4.1.3 Change of Password

The Vendors are recommended to change their password at an interval of 3 months although the system would not guard against this. To change the password, Vendors can issue CHNGPWDREQ command through their system with existing password and new password. Both existing and new passwords are encrypted by session key obtained during logon process using Triple-DES algorithm (please see Appendix C for details). As before, the encrypted password should be transformed to Base64 format. After verifying the correctness of the existing password, IIS responds with CHNGPWDRESP to indicate if the changes are effective in IIS. The following response status can be found.

Response status	Additional information / Error Code	Description
SUCCESS		Successful status
FAILURE	INVALID_MESSAGE	Invalid message format
FAILURE	INCORRECT_SUBSCRIBER	Incorrect Vendor identity or password
FAILURE	INVALID_PASSWORD	Password is malformed (i.e. invalid character exists or length of password < 6) OR historical password is used.
FAILURE	PERMISSION_DROP	Operation not allowed because permission is dropped
FAILURE	SESSION_NOT_ESTABLISHED	Cannot perform this function since session is not established
FAILURE	SERVICE_NOT_AVAILABLE	Service not available

A session must be established before this command can be issued.

4.1.4 Headline Recovery

The Vendor can request two kinds of headline recovery, full and partial, after logging onto IIS. Full headline recovery command FULLRECVYREQ is to rebuild a total of 1-day's headline. Partial headline recovery command PARTRECVYREQ with "Headline sequence number" is to rebuild all those headlines subsequent to this sequence number. IIS would respond with RECVYRESP with number of recovery headline to be sent to the Vendor.

During headline recovery, headlines are sent in a reverse chronological order. It should be noted that the most recent headline is also sent simultaneously to the Vendor during headline recovery. After all pieces of the recovery headline are sent, IIS sends an unsolicited message RECVYCOMPLETE to inform the Vendor the completion of the headline recovery.

The following is the request commands for headline recovery.

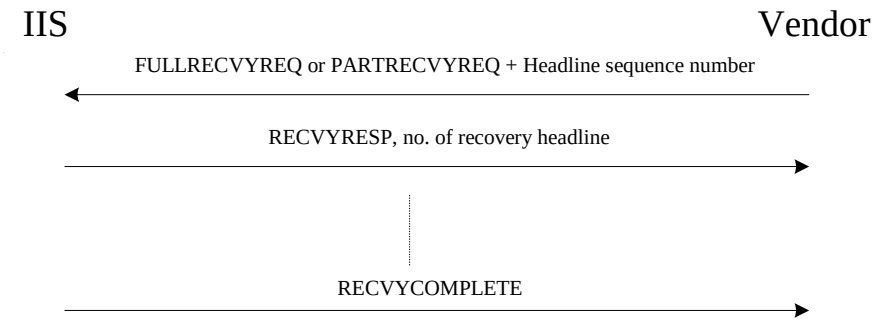
Request command	Additional information	Description
FULLRECVYREQ		Request 1-day online headline recovery
PARTRECVYREQ	Headline sequence number	Request recovery headlines which come after the one specified by headline sequence number

The following response status RECVYRESP can be found.

Response status	Additional information/ Error code	Description
SUCCESS	Number of recovery headline	Successful status
FAILURE	INVALID_MESSAGE	Invalid message format
FAILURE	PERMISSION_DROP	Operation not allowed because permission is dropped
FAILURE	SESSION_NOT_ESTABLISHED	Cannot perform this function since session is not established
FAILURE	NEWS_NOT_FOUND	Supplied Headline Sequence Number cannot be located in IIS.
FAILURE	SYSTEM_BUSY	The new request cannot be fulfilled because IIS is still processing recovery request
FAILURE	SERVICE_NOT_AVAILABLE	Service not available

The following is the unsolicited command to indicate the completion of the recovery headline.

Unsolicited command	Additional information	Description
RECVYCOMPLETE		To inform the Vendor that headline recovery is completed



4.1.5 Permission dropped

In cases where service to a Vendor has been suspended, the Vendor will receive PERMISSIONDROP unsolicited command message.

Unsolicited command	Additional information	Description
PERMISSIONDROP		To inform the Vendor that its identity cannot be used to access IIS service

Afterwards, the system will automatically disconnect the existing session.

4.1.6 Exceptional Handling

“SERVICE_NOT_AVAILABLE” status reveals that some of the components in IIS cannot be communicated. Thus, there may not be updated headline and logon mechanism may not be able to be accomplished. The Vendor should drop TCP/IP connection and try to connect to IIS for every 15 minutes.

On processing headline recovery request, IIS ignores new headline recovery request command with same unique request identity “ReqID”. If the request identity is different, IIS responds with “SYSTEM_BUSY” status.

On the other hand, if there is no response from IIS within 30 seconds after a command has been sent, the Vendor should re-send the command with same unique request identity again. If no response is received, it

is recommended to drop TCP/IP connection and then establish the TCP/IP connection again. Vendor should reconnect to IIS system once disconnection detected and keep the service outage within 5 minutes. Vendor is recommended to perform full recovery after reconnection in order to recover the lost IIS news and minimize the latency of receiving IIS news. Please make sure that the network connectivity between IIS and Vendor is fine and TCP/IP connection is established.

Annual drill for line failure reconnection will be arranged by Exchange and the test result will be published on HKEx website for public reference.

4.2 Data messages

There are only one type of data message - headline.

4.2.1 Headline

Vendor will receive a UPDATEHEADLINE message for the most recent headline and a RECVYHEADLINE message for the recovery headline. Both messages can contain Unique Headline Identity, date/time, subtype, product categories, language, headline content, encoding format of the headline content. For UPDATEHEADLINE, a sequence number is assigned by IIS and this sequence number "Headline Sequence Number" is used for partial headline recovery.

There is a "Type" attribute defined in the UPDATEHEADLINE tag: [ALERT]/[FIRSTTAKE]/[SUBTAKE]/[CANCELLED]. More detailed explanation is found in next section.

4.3 Control flow message

Control flow message is used to ensure that the communication between IIS and the Vendor is working properly. There is one message type – status enquiry.

4.3.1 Status enquiry

In general, IIS would issue STATUSREQ command to the Vendor if there is no traffic in both directions between IIS and Vendor for 120 seconds. Then the Vendor should respond with STATUSRESP status. If IIS does not receive this status response for another 120 seconds, it would issue the command again. After 120 seconds from the second STATUSREQ command, IIS disconnects the session by dropping the TCP/IP connection. Conversely, the Vendor can also issue STATUSREQ command to find out if IIS is working or not. The same format of STATUSRESP status response should be received. It is recommended for the Vendor to issue this command only when it does not receive any message from IIS for 60 seconds.

4.4 General exception

When the Vendor receives message that cannot be recognized as one of the above message codes or the message is an incomplete XML message, it should discard the message. If the Vendor receives 3 consecutive invalid messages, it is recommended to drop the existing TCP/IP connections and connect to IIS again. Similarly, when IIS receives 3 sequential invalid messages, it would drop TCP/IP connection automatically.

5. Detailed Message Format

The message format for each message code in details is described in this section. The XML schema can be found in the Appendix A for reference.

5.1 Command and Response Messages

The format of command status response is shown as follows.

```
<Status>
	<Success />
	<Failure>
		<ErrCode>NNNNN</ErrCode>
		<ErrMsg>[X]*</ErrMsg>
	</Failure>
</Status>
```

Tag	Format	M/O	Occurs	Description	Attributes	Format	M/O	Description
Status	complex	M	1	Response status				
Success	N/A	O	1	command is succeeded				
Failure	complex	O	1	command is failed				
ErrCode	[N]*5	O	1	Error code				
ErrMsg	[X]*	O	1	Error Message				

The <Success> tag indicates the command is successfully executed while the <Failure> tag indicates the command is failure to execute with <ErrCode> and <ErrMsg> explaining the reason. Either one of <Success> or <Failure> tags included in a <Status> tag.

5.1.1 INITREQ

```
<?xml version="1.0" encoding="UTF-8"?>
<NDSML xmlns="http://www.hkex.com.hk/iis">
	<MsgHeader>
		<MsgDate>20021223T050413+0800</MsgDate>
		<MsgID>INITREQ</MsgID>
		<MsgType>NDScmd</MsgType>
	</MsgHeader>
	<INITREQ ReqId="99999"/>
</NDSML>
```

Tag	Format	M/O	Occurs	Description	Attributes	Format	M/O	Description
INITREQ	N/A	M	1	Initialization request message	ReqId	[N]*5	M	request id used to be mapped with its response

5.1.2 INITRESP

```
<?xml version="1.0" encoding="UTF-8"?>
<NDSML xmlns="http://www.hkex.com.hk/iis">

	<MsgHeader>
		<MsgDate>20021223T050413+0800</MsgDate>
		<MsgID>INITRESP</MsgID>
		<MsgType>NDScmd</MsgType>
	</MsgHeader>
```

```
      <INITRESP ReqId="99999">
            <Status>
                  <Success />
                  <Failure>
                        <ErrCode>NNNNN</ErrCode>
                        <ErrMsg>[X]*</ErrMsg>
                  </Failure>
            </Status>
            <SessionKey>
                  <Encoding Notation="Base64">
                        <Encoding Notation="3DES">
                              <DataContent>[X]*</DataContent>
                        </Encoding>
                  </Encoding>
            </SessionKey>
      </INITRESP>
</NDSML>
```

Tag	Format	M/O	Occurs	Description	Attributes	Format	M/O	Description
INITRESP	complex	M	1	Initialization response message	ReqId	[N]*5	M	used to be mapped with its request
For success status:								
SessionKey	Complex	O	1	IIS Session key				
Encoding:1	Complex	M	1	Encoding of the Session key	Notation	Base64	M	Encoding Method (Base64)
Encoding:2	Complex	M	1	Encoding of the Session key in big-Endian format	Notation	3DES	M	Encoding Method (3DES)
DataContent	[X]*	M	1	Session key's data				

5.1.3 LOGONREQ

```
<?xml version="1.0" encoding="UTF-8"?>
<NDSML xmlns="http://www.hkex.com.hk/iis">
      <MsgHeader>
            <MsgDate>20021223T050413+0800</MsgDate>
            <MsgID>LOGONREQ</MsgID>
            <MsgType>NDScmd</MsgType>
      </MsgHeader>
      <LOGONREQ ReqId="99999">
            <Username>XXXXXXXX</Username>
            <Password>
                  <Encoding Notation="Base64">
                        <Encoding Notation="3DES">
                              <DataContent>[X]*</DataContent>
                        </Encoding>
                  </Encoding>
            </Password>
      </LOGONREQ>
</NDSML>
```

Tag	Format	M/O	Occurs	Description	Attributes	Format	M/O	Description
LOGONREQ	complex	M	1	Logon command	ReqId	[N]*5	M	To be mapped with its response
Logon Parameters:								
Username	[X]*10	M	1	Vendor identity				

Password	complex	M	1	Vendor password encrypted by IIS Session key				
Encoding:1	complex	M	1	Encoding of the password	Notation	Base64	M	Encoding Method (Base64)
Encoding:2	complex	M	1	Encoding of the password	Notation	3DES	M	Encoding Method (3DES)
DataContent	[X]*	M	1	Password's data				

5.1.4 LOGONRESP

```
<?xml version="1.0" encoding="UTF-8"?>
<NDSML xmlns="http://www.hkex.com.hk/iis">
      <MsgHeader>
            <MsgDate>20021223T050413+0800</MsgDate>
            <MsgID>LOGONRESP</MsgID>
            <MsgType>NDScmd</MsgType>
      </MsgHeader>
      <LOGONRESP ReqId="99999">
            <Status>
                  <Success />
                  <Failure>
                        <ErrCode>NNNNN</ErrCode>
                        <ErrMsg>[X]*</ErrMsg>
                  </Failure>
            </Status>
            <ServiceType>[HDL/HDL+ATT]</ServiceType>
            <PackageType>[A/B/C]+</PackageType>
            <LastLoginTime>20021221T030345+0800</LastLoginTime>
      </LOGONRESP>
</NDSML>
```

Tag	Format	M/O	Occurs	Description	Attributes	Format	M/O	Description
LOGONRESP	complex	M	1	Logon response message	ReqId	[N]*5	M	To be mapped with its request
For success status:								
ServiceType	HDL/HDL +ATT	M	1	Service Type				
PackageType	A/B/C..	M	1	Subscribed package type				
LastLoginTime	CCYYMMDDT24HHMISS[+-]NNNN	M	1	Last logon time				

5.1.5 LOGOFF

```
<?xml version="1.0" encoding="UTF-8"?>
<NDSML xmlns="http://www.hkex.com.hk/iis">
      <MsgHeader>
            <MsgDate>20021223T050413+0800</MsgDate>
            <MsgID>LOGOFF</MsgID>
            <MsgType>NDScmd</MsgType>
      </MsgHeader>
      <LOGOFF/>
</NDSML>
```

Tag	Format	M/O	Occurs	Description
LOGOFF	N/A	M	1	Logoff command

5.1.6 CHNGPWDREQ

```
<?xml version="1.0" encoding="UTF-8"?>
<NDSML xmlns="http://www.hkex.com.hk/iis">
      <MsgHeader>
            <MsgDate>20021223T050413+0800</MsgDate>
            <MsgID>CHNGPWDREQ</MsgID>
            <MsgType>NDScmd</MsgType>
      </MsgHeader>
      <CHNGPWDREQ ReqId="99999">
            <Password>
                  <Encoding Notation="Base64">
                        <Encoding Notation="3DES">
                              <DataContent>[X]*</DataContent>
                        </Encoding>
                  </Encoding>
            </Password>
            <NewPassword>
                  <Encoding Notation="Base64">
                        <Encoding Notation="3DES">
                              <DataContent>[X]*</DataContent>
                        </Encoding>
                  </Encoding>
            </NewPassword>
      </CHNGPWDREQ>
</NDSML>
```

Tag	Format	M/O	Occurs	Description	Attributes	Format	M/O	Description
CHNGPWDREQ	complex	M	1	Change password command	ReqId	[N]*5	M	To be mapped with its response
Request Parameters:								
Password	complex	M	1	Vendor old password encrypted by IIS Session key				
Encoding:1	complex	M	1	Encoding of the password	Notation	Base64	M	Encoding Method (Base64)
Encoding:2	complex	M	1	Encoding of the password	Notation	3DES	M	Encoding Method (3DES)
DataContent	[X]*	M	1	Password's data				
NewPassword	complex	M	1	Vendor new password encrypted by IIS Session key				
Encoding:1	complex	M	1	Encoding of the password	Notation	Base64	M	Encoding Method (Base64)
Encoding:2	complex	M	1	Encoding of the password	Notation	3DES	M	Encoding Method (3DES)
DataContent	[X]*	M	1	Password's data				

5.1.7 CHNGPWDRESP

```
<?xml version="1.0" encoding="UTF-8"?>
<NDSML xmlns="http://www.hkex.com.hk/iis">
      <MsgHeader>
            <MsgDate>20021223T050413+0800</MsgDate>
            <MsgID>CHNGWDRESP</MsgID>
```

```
            <MsgType>NDScmd</MsgType>
      </MsgHeader>
      <CHNGPWDRESP ReqId="99999">
            <Status>
                  <Success />
                  <Failure>
                        <ErrCode>NNNNN</ErrCode>
                        <ErrMsg>[X]*</ErrMsg>
                  </Failure>
            </Status>
      </CHNGPWDRESP>
</NDSML>
```

Tag	Format	M/O	Occurs	Description	Attributes	Format	M/O	Description
CHNGPWDRESP	complex	M	1	Change password response message	ReqId	[N]*5	M	To be mapped with its request

5.1.8 FULLRECVYREQ

```
<?xml version="1.0" encoding="UTF-8"?>
<NDSML xmlns="http://www.hkex.com.hk/iis">
      <MsgHeader>
            <MsgDate>20021223T050413+0800</MsgDate>
            <MsgID>FULLRECVYREQ</MsgID>
            <MsgType>NDScmd</MsgType>
      </MsgHeader>
      <FULLRECVYREQ ReqId="99999"/>
</NDSML>
```

Tag	Format	M/O	Occurs	Description	Attributes	Format	M/O	Description
FULLRECVYREQ	N/A	M	1	Request for full recovery command	ReqId	[N]*5	M	To be mapped with its response

5.1.9 PARTRECVYREQ

```
<?xml version="1.0" encoding="UTF-8"?>
<NDSML xmlns="http://www.hkex.com.hk/iis">
      <MsgHeader>
            <MsgDate>20021223T050413+0800</MsgDate>
            <MsgID>PARTRECVYREQ</MsgID>
            <MsgType>NDScmd</MsgType>
      </MsgHeader>
      <PARTRECVYREQ ReqId="99999">
            <NewsSeqNo>9999999999</NewsSeqNo>
      </PARTRECVYREQ>
</NDSML>
```

Tag	Format	M/O	Occurs	Description	Attributes	Format	M/O	Description
PARTRECVYREQ	N/A	M	1	Request for partial recovery command	ReqId	[N]*5	M	To be mapped with its response
NewsSeqNo	[9]*10	M	1	Last sequence number of the headline received				

5.1.10 RECVYRESP

```
<?xml version="1.0" encoding="UTF-8"?>
<NDSML xmlns="http://www.hkex.com.hk/iis">
      <MsgHeader>
            <MsgDate>20021223T050413+0800</MsgDate>
            <MsgID>RECVYRESP</MsgID>
            <MsgType>NDScmd</MsgType>
      </MsgHeader>
      <RECVYRESP ReqId="99999">
            <Status>
                  <Success />
                  <Failure>
                        <ErrCode>NNNNN</ErrCode>
                        <ErrMsg>[X]*</ErrMsg>
                  </Failure>
            </Status>
            <NoofNewsItem>999</NoofNewsItem>
      </RECVYRESP>
</NDSML>
```

Tag	Format	M/O	Occurs	Description	Attributes	Format	M/O	Description
RECVYRESP	complex	M	1	Full recovery/ Partial recovery response	ReqId	[N]*5	M	used to be mapped with its request
For Success Status :								
NoofNewsItem	[9]*3	O	1	Number of recovered headlines				

5.1.11 RECVYCOMPLETE

```
<?xml version="1.0" encoding="UTF-8"?>
<NDSML xmlns="http://www.hkex.com.hk/iis">
      <MsgHeader>
            <MsgDate>20021223T050413+0800</MsgDate>
            <MsgID>RECVYCOMPLETE</MsgID>
            <MsgType>NDScmd</MsgType>
      </MsgHeader>
      <RECVYCOMPLETE ReqId="99999"/>
</NDSML>
```

Tag	Format	M/O	Occurs	Description	Attributes	Format	M/O	Description
RECVYCOMPLETE	N/A	M	1	Notification to Vendor for recovery completeness	ReqId	[N]*5	M	used to be mapped with its request

5.1.12 PERMISSIONDROP

```
<?xml version="1.0" encoding="UTF-8"?>
<NDSML xmlns="http://www.hkex.com.hk/iis">
      <MsgHeader>
            <MsgDate>20021223T050413+0800</MsgDate>
            <MsgID>PERMISSIONDROP</MsgID>
            <MsgType>NDScmd</MsgType>
      </MsgHeader>
```

```
      <PERMISSIONDROP>
            <Reason>[X]*</Reason>
      </PERMISSIONDROP>
</NDSML>
```

Tag	Format	M/O	Occurs	Description
PERMISSIONDROP	N/A	M	1	Notification to Vendor that their permission is revoked.
Reason	[X]*	M	1	The reason why Vendor's permission is dropped

5.2 Data Messages

5.2.1 UPDATEHEADLINE and RECVYHEADLINE

These two types of headline share the same format except that the content is enclosed by <UPDATEHEADLINE> and <RECVYHEADLINE> tags for updated and recovery headline respectively.

The following is an example of UPDATEHEADLINE.

```
<?xml version="1.0" encoding="UTF-8"?>
<NDSML xmlns="http://www.hkex.com.hk/iis">
      <MsgHeader>
            <MsgDate>20021223T050413+0800</MsgDate>
            <MsgID>UPDATEHEADLINE</MsgID>
            <MsgType>NDSdata</MsgType>
      </MsgHeader>
      <UPDATEHEADLINE Type="FIRSTTAKE" SeqNo="9999999999">
             <NewsML>
               <NewsItem>
                  <NewsIdentifier>
                     <ProviderId>HKEX-XXX</ProviderId>
                     <DateId>20021223</DateId>
                     <NewsItemId>[X]*</NewsItemId>
                  </NewsIdentifier>
                     <DescriptiveMetadata>
                        <Language FormalName="XX-XX"/>
                        <SubjectCode>
                           <SubjectMatter FormalName="[X]*" Scheme="[X]*"/>
                        </SubjectCode>
                     </DescriptiveMetadata>
                     <NewsComponent>
                        <NewsLines>
                           <DateLine>20021223T050413+0800</DateLine>
                           <HeadLine>
                              <Encoding Notation="Base64">
                                 <DataContent>[X]*</DataContent>
                              </Encoding>
                           </HeadLine>
                        </NewsLines>
                  </NewsComponent>
               </NewsItem>
            </NewsML>
      </UPDATEHEADLINE>
</NDSML>
```

For recovery headline, the tag <UPDATEHEADLINE> is replaced by <RECVYHEADLINE>.

In either type of headline, there is one field called subtype which is used to identify types of headline. The following table summarizes the types of headline.

Subtype	Description
FIRSTTAKE	Indicating that this is the first time IIS has received this headline and it contains headline content and news information
CANCELLED	Indicating that the headline identified by <NewsIdentifier> is cancelled in the news source.
AMENDED	Indicating that the headline identified by <NewsIdentifier> is an amended news in the news source.

For CANCELLED subtype, it is up to the Vendor to remove the news or not while the headline content indicates that this headline is cancelled. This headline is still sent during recovery.

Upon data recovery, the Vendor will receive the latest headlines. In this case, the cancelled headline will be received earlier than the original headline that were cancelled after Vendor has performed data recovery or when IIS has just switched from the Primary Site to Disaster Recovery Site, or vice versa.

Amendment of Headline Category – where only Headline Category in the news was amended. Same as amended news, Vendor will receive a CANCELLED message with the news identity indicating the original version of the news that is being amended. An AMENDED message with a new news identity and new Headline Categories is then sent to Vendor after the CANCELLED message. Vendor can co-relate the amended version of the news and the original version of the amended news by using the news title. News title will remain unchanged even Headline Category (T1 or T2) is changed during the amendment process. Upon data recovery, Vendor will receive the latest headlines first. Hence, Vendor will receive AMENDED message and followed with the CANCELLED message. However, in this case, the original FIRSTTAKE message with the original version of the amended news is not provided. This will happen after Vendor has performed data recovery or when IIS has just switched from the Primary Site to Disaster Recovery Site, or vice versa.

For illustration, the following examples depict how AMENDED message will work under normal and recovery processes. All messages are listed in order of time sequence when the message is received by Vendor.

Amendment of Headline Category (**for immediate released news**)

Order	Message Type	Message Property
1	FIRSTTAKE	News ID=1000 Headline Category-T1=10000 Headline Category-T2=20000 Headline Category-T2=20001
2	CANCELLED	News ID=1000 Headline Category-T1=10000 Headline Category-T2=20000 Headline Category-T2=20001
3	AMENDED	News ID=2000 Headline Category-T1=40000 Headline Category-T2=50000 Headline Category-T2=50001

Amendment of Headline Category (**for immediate released news** during Recovery Process)

Order	Message Type	Message Property
1	AMENDED	News ID=2000 Headline Category-T1=40000 Headline Category-T2=50000 Headline Category-T2=50001
2	CANCELLED	News ID=1000 Headline Category-T1=10000 Headline Category-T2=20000 Headline Category-T2=20001

For some business reasons, some news may be hold up and released at specific time. If any modification such as cancellation and headline amendment may be applied to these pending news and the possible message sequence is shown as follow:

Amendment of Headline Category (for hold up original news and immediate released amended news)

Order	Message Type	Message Property
1	FIRSTTAKE **Hold up by IIS and will not deliver to Vendor**	News ID=1000 Headline Category-T1=10000 Headline Category-T2=20000 Headline Category-T2=20001
3	AMENDED	News ID=2000 Headline Category-T1=40000 Headline Category-T2=50000 Headline Category-T2=50001
5	CANCELLED **Release to Vendor at specific time and later than the above mentioned AMENDED and related SUBTAKE**	News ID=1000 Headline Category-T1=10000 Headline Category-T2=20000 Headline Category-T2=20001

Amendment of Headline Category (for hold up original news and immediate released amended news during recovery)

Order	Message Type	Message Property
1	AMENDED	News ID=2000 Headline Category-T1=40000 Headline Category-T2=50000 Headline Category-T2=50001
3	CANCELLED	News ID=1000 Headline Category-T1=10000 Headline Category-T2=20000 Headline Category-T2=20001

Amendment of Headline Category (for hold up original news and canelled news before release)

Order	Message Type	Message Property
1	FIRSTTAKE **Hold up by IIS and will not deliver to Vendor**	News ID=1000 Headline Category-T1=10000 Headline Category-T2=20000 Headline Category-T2=20001
3	CANCELLED **Release to Vendor at**	News ID=1000 Headline Category-T1=10000 Headline Category-T2=20000

	specific time	Headline Category-T2=20001

Amendment of Headline Category (for hold up original news and canelled news before release during recovery)

Order	Message Type	Message Property
3	CANCELLED	News ID=1000 Headline Category-T1=10000 Headline Category-T2=20000 Headline Category-T2=20001

Note:
In addition to CANCELLED and AMENDED message for current day news, it is possible for Vendor to received any CANCELLED and AMENDED message for past news.

The unique identity of news is revealed by <ProviderId>, <DateId> and <NewsItemId>. The news information such as document type code (category) and stock code are found within <DescriptiveMetadata> tag. There are four types of subject code within <DescriptiveMetadata> and these include category code (or called Headline Category), market code, stock code, stock name, and expiry date. Category code identifies the category of the information, e.g. company profile or financial report. Market code reveals what markets the information is related to, e.g. GEM board. Multiple numbers of <SubjectMatter> tags can be found in one headline summary. Expiry date identifies the news expiry date*. The news should not be sent out if current date greater than the expiry date. Please refer to appendix F for mapping and example.

*News expiry date: certain announcements will be kept releasing on various channels, e.g. HKEx web, AMS & MDF repeatedly for a certain period whereas those announcements will only be released once in IIS, but with an expiry date for Vendors to identify and replicate those news for their subscribers before the expiry date, if they wish.

A headline sequence number is assigned to each headline sent from. This sequence number is used for partial headline recovery. Thus, same unique identity of news as mentioned would have different sequence number for different kinds of subtype. The sequence number of recovery headline for same update headline is the same.

Tag	Format	M/O	Occurs	Description	Attributes	Format	M/O	Description
UPDATEHEADLINE	complex	M	1	News Headline Message	Type	ALERT/ FIRSTTAKE/ SUBTAKE/ CANCELLED/ CONTINGENCY	M	Subtype of the headline
					SeqNo	[9]*10	M	Unique identifier of this message
NewsML	complex	M	1	News Markup language (by IPTC)				
NewsItem	complex	M	1	News Item				
NewsIdentitifier	complex	M	1	The news identifier in IIS				
ProviderID	HKEX-XXX	M	1	Provider of the news. Possible values: HKEX-EPS, HKEX-EXN, HKEX-MND				
DateID	CCYYMMDD	M	1	Issue date of the news				
NewsItemId	[X]*	M	1	News Item sequence no				
DescriptiveMetadata	complex	O	1	New Item Descriptive data				
Language	complex	O	1	Language of news headline	FormalName	XX-XX ISO 639 Language	M	ISO language code

						code – ISO 3166 country code		
SubjectCode	complex	O	1	Classification keywords				
SubjectMatter	N/A	O	*	keyword describing the news	FormalName	[Category code]	M	Category code of IIS for classifying the news
					Scheme	Naming Scheme	O	Naming scheme of FormalName attribute.
NewsComponent	complex	M	1	News content				
NewsLines	complex	M	1	News Header				
HeadLine	complex	M	1	News Headline				
Encoding:1	complex	M	1	Encoding of the data content	Notation	[x]*	M	Encoding Method (Base64)
DataContent	[X]*	M	1	Headline's data				

As before, for recovery headline, the tag <UPDATEHEADLINE> is replaced by <RECVYHEADLINE>.

5.3 Control Flow Messages

5.3.1 STATUSREQ

```
<?xml version="1.0" encoding="UTF-8"?>
<NDSML xmlns="http://www.hkex.com.hk/iis">
      <MsgHeader>
            <MsgDate>20021223T050413+0800</MsgDate>
            <MsgID>STATUSREQ</MsgID>
            <MsgType>NDSctrl</MsgType>
      </MsgHeader>
      <STATUSREQ ReqId="99999"/>
</NDSML>
```

Tag	Format	M/O	Occurs	Description	Attributes	Format	M/O	Description
STATUSREQ	Complex	M	1	Connection Status enquiry	ReqId	[N]*5	M	used to be mapped with its response

5.3.2 STATUSRESP

```
<?xml version="1.0" encoding="UTF-8"?>
<NDSML xmlns="http://www.hkex.com.hk/iis">
      <MsgHeader>
            <MsgDate>20021223T050413+0800</MsgDate>
            <MsgID>STATUSRESP</MsgID>
            <MsgType>NDSctrl</MsgType>
      </MsgHeader>
      <STATUSRESP ReqId="99999"/>
</NDSML>
```

Tag	Format	M/O	Occurs	Description	Attributes	Format	M/O	Description
STATUSRESP	Complex	M	1	Connection Status enquiry response	ReqId	[N]*5	M	used to be mapped with its request

6. SECURITY AND CONTROL

IIS does not force the expiry of the vendor password. However, IIS vendors are recommended to change their password at an interval of 3 months for security reasons though the system would not guard against this.

The Exchange's network has applied different levels of security measures to provide a secure infrastructure for the Issuer Information *feed* Service (IIS) System. All network routers and LAN switches are password protected. The password protection has restricted access to network components.

Packet filtering is applied in all core routers within the network. Filtering rules are configured consistently in all routers throughout the path from Vendors' sites to IIS host system and the network only allows traffic to travel in pre-defined paths. Any attempt from a Vendors' site to connect with other un-predefined network components or another peer Vendor's site will be blocked.

Static routing is applied for traffic between the Vendors' sites and the core network of the Exchange. The core network routers never accept routing updates from the Vendor's site routers as no routing protocol is running at these WAN interfaces. Static routes are configured for Vendor's routers. Only routes to the Exchange's host site networks are configured.

The network will ride on the Exchange's Securities and Derivatives Network (SDNet) in the form of virtual private network. With the provision of private LAN (VLAN), only pre-defined network access points can communicate with each other.

Appendix A XML Schema for Message Validation

This is for reference only. The actual XML schema is to be delivered by the Exchange through email.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- edited with XML Spy v4.1 U (http://www.xmlspy.com) -->
<xsd:schema targetNamespace="http://www.hkex.com.hk/iis" xmlns="http://www.hkex.com.hk/iis"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
    <xsd:simpleType name="gmtDateTime">
        <xsd:restriction base="xsd:string">
            <xsd:pattern value="20[0-9][0-9](0[1-9]|1[0-2])(0[1-9]|[1-2][0-9]|3[0-1])(T([0-1][0-9]|2[0-3])([0-5][0-9][0-
5][0-9]|2400)([+-](0[0-9]|1[0-1])([0-5][0-9]|1200))?)?"/>
        </xsd:restriction>
    </xsd:simpleType>
    <xsd:simpleType name="mesgType">
        <xsd:restriction base="xsd:string">
            <xsd:enumeration value="NDScmd"/>
            <xsd:enumeration value="NDSctrl"/>
            <xsd:enumeration value="NDSdata"/>
        </xsd:restriction>
    </xsd:simpleType>
    <xsd:simpleType name="services">
        <xsd:restriction base="xsd:string">
            <xsd:enumeration value="HDL"/>
        </xsd:restriction>
    </xsd:simpleType>
    <xsd:simpleType name="long">
        <xsd:restriction base="xsd:integer">
            <xsd:minInclusive value="0"/>
            <xsd:maxInclusive value="9999999999"/>
        </xsd:restriction>
    </xsd:simpleType>
    <xsd:simpleType name="quantity">
        <xsd:restriction base="xsd:integer">
            <xsd:minInclusive value="0"/>
            <xsd:maxInclusive value="99999"/>
        </xsd:restriction>
    </xsd:simpleType>
    <xsd:simpleType name="segment">
        <xsd:restriction base="xsd:integer">
            <xsd:minInclusive value="0"/>
            <xsd:maxInclusive value="9999"/>
        </xsd:restriction>
    </xsd:simpleType>
    <xsd:simpleType name="userid">
        <xsd:restriction base="xsd:string">
            <xsd:minLength value="1"/>
            <xsd:maxLength value="10"/>
        </xsd:restriction>
    </xsd:simpleType>
    <xsd:simpleType name="errcde">
        <xsd:restriction base="xsd:string">
            <xsd:pattern value="[1-9][0-9][0-9][0-9][0-9]"/>
        </xsd:restriction>
    </xsd:simpleType>
    <xsd:simpleType name="id">
        <xsd:restriction base="xsd:string">
            <xsd:pattern value="[0-9][0-9][0-9][0-9][0-9]"/>
        </xsd:restriction>
    </xsd:simpleType>
    <xsd:simpleType name="dateonly">
        <xsd:restriction base="xsd:string">
            <xsd:pattern value="20[0-9][0-9](0[1-9]|1[0-2])(0[1-9]|[1-2][0-9]|3[0-1])"/>
        </xsd:restriction>
    </xsd:simpleType>
    <xsd:simpleType name="provider">
        <xsd:restriction base="xsd:string">
            <xsd:enumeration value="HKEX-EPS"/>
            <xsd:enumeration value="HKEX-EXN"/>
            <xsd:enumeration value="HKEX-MND"/>
        </xsd:restriction>
```

```
    </xsd:simpleType>
    <xsd:simpleType name="newsItemid">
    <xsd:restriction base="xsd:string" />
    </xsd:simpleType>
    <xsd:element name="DataContent">
        <xsd:complexType>
            <xsd:simpleContent>
                <xsd:extension base="xsd:string">
                    <xsd:attribute name="Segment" type="id"/>
                </xsd:extension>
            </xsd:simpleContent>
        </xsd:complexType>
    </xsd:element>
    <xsd:group name="SingleEncodedData">
        <xsd:sequence>
            <xsd:element name="Encoding">
                <xsd:complexType>
                    <xsd:sequence>
                        <xsd:element ref="DataContent"/>
                    </xsd:sequence>
                    <xsd:attribute name="Notation" type="xsd:string" use="required"/>
                </xsd:complexType>
            </xsd:element>
        </xsd:sequence>
    </xsd:group>
    <xsd:element name="Failure">
        <xsd:annotation>
            <xsd:documentation>
=================================== Failure ===================================
Failure Status
================================================================================
            </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType>
            <xsd:sequence>
                <xsd:element name="ErrCode" type="errcde"/>
                <xsd:element name="ErrMsg" type="xsd:string"/>
            </xsd:sequence>
        </xsd:complexType>
    </xsd:element>
    <xsd:element name="Status">
        <xsd:annotation>
            <xsd:documentation>
=================================== Status ====================================
Response Result
================================================================================
            </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType mixed="true">
            <xsd:choice>
                <xsd:element name="Success" type="xsd:string"/>
                <xsd:element ref="Failure"/>
            </xsd:choice>
        </xsd:complexType>
    </xsd:element>
    <xsd:element name="MsgHeader">
        <xsd:annotation>
            <xsd:documentation>
================================= MsgHeader ==================================
Header Information of IIS message.
================================================================================
            </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType>
            <xsd:sequence>
                <xsd:element name="MsgDate" type="gmtDateTime"/>
                <xsd:element name="MsgID" type="xsd:string"/>
                <xsd:element name="MsgType" type="mesgType"/>
            </xsd:sequence>
        </xsd:complexType>
    </xsd:element>
    <xsd:element name="NewsIdentifier">
```

```
        <xsd:annotation>
            <xsd:documentation>
================================== NewsIdentifier ==================================
A globally unique identifier for a NewsItem.
====================================================================================

            </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType>
            <xsd:sequence>
                <xsd:element name="ProviderId" type="provider"/>
                <xsd:element name="DateId" type="dateonly"/>
                <xsd:element name="NewsItemId" type="newsItemid"/>
            </xsd:sequence>
        </xsd:complexType>
    </xsd:element>
    <xsd:element name="NewsItem">
        <xsd:annotation>
            <xsd:documentation>
================================== NewsItem ==================================
Modified NewsML
==============================================================================

            </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType>
            <xsd:sequence>
                <xsd:element ref="NewsIdentifier"/>
                <xsd:element ref="DescriptiveMetadata" minOccurs="0"/>
                <xsd:element ref="NewsComponent"/>
            </xsd:sequence>
        </xsd:complexType>
    </xsd:element>
    <xsd:element name="DescriptiveMetadata">
        <xsd:annotation>
            <xsd:documentation>
============================== DescriptiveMetadata==================================
List of Stock code, subject code, announcement type etc.
==============================================================================

            </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType>
            <xsd:sequence>
                <xsd:element name="Language">
                    <xsd:complexType>
                        <xsd:attribute name="FormalName" type="xsd:string" use="required"/>
                        <xsd:attribute name="Scheme" type="xsd:string"/>
                    </xsd:complexType>
                </xsd:element>
                <xsd:element name="SubjectCode">
                    <xsd:complexType>
                        <xsd:sequence>
                            <xsd:element name="SubjectMatter" maxOccurs="unbounded">
                                <xsd:complexType>
                                    <xsd:attribute name="FormalName" type="xsd:string" use="required"/>
                                    <xsd:attribute name="Scheme" type="xsd:string"/>
                                </xsd:complexType>
                            </xsd:element>
                        </xsd:sequence>
                    </xsd:complexType>
                </xsd:element>
            </xsd:sequence>
        </xsd:complexType>
    </xsd:element>
    <xsd:element name="NewsLines">
        <xsd:annotation>
            <xsd:documentation>
============================== NewsLines ==================================
News Headline
==========================================================================

            </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType>
```

```
            <xsd:sequence>
                <xsd:element name="DateLine" type="gmtDateTime"/>
                <xsd:element name="HeadLine">
                    <xsd:complexType>
                        <xsd:sequence>
                            <xsd:group ref="SingleEncodedData"/>
                        </xsd:sequence>
                    </xsd:complexType>
                </xsd:element>
            </xsd:sequence>
        </xsd:complexType>
    </xsd:element>
    <xsd:element name="NewsML">
        <xsd:annotation>
            <xsd:documentation>
==================================== NewsML ====================================
Modified NewsML
================================================================================
            </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType>
            <xsd:sequence>
                <xsd:element ref="NewsItem"/>
            </xsd:sequence>
        </xsd:complexType>
    </xsd:element>
    <xsd:element name="LOGONREQ">
        <xsd:annotation>
            <xsd:documentation>
==================================== LOGONREQ ==================================
Vendor Logon command message
================================================================================

            </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType>
            <xsd:sequence>
                <xsd:element name="Username" type="userid"/>
                <xsd:element name="Password">
                    <xsd:complexType>
                        <xsd:sequence>
                            <xsd:element name="Encoding">
                                <xsd:complexType>
                                    <xsd:group ref="SingleEncodedData"/>
                                    <xsd:attribute name="Notation" type="xsd:string" use="required"/>
                                </xsd:complexType>
                            </xsd:element>
                        </xsd:sequence>
                    </xsd:complexType>
                </xsd:element>
            </xsd:sequence>
            <xsd:attribute name="ReqId" type="quantity" use="required"/>
        </xsd:complexType>
    </xsd:element>
    <xsd:element name="LOGONRESP">
        <xsd:annotation>
            <xsd:documentation>
================================== LOGONRESP ===================================
Vendor Logon command response
================================================================================
            </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType>
            <xsd:sequence>
                <xsd:element ref="Status"/>
                <xsd:element name="ServiceType" type="services" minOccurs="0"/>
                <xsd:element name="PackageType" type="xsd:string" minOccurs="0"/>
                <xsd:element name="LastLoginTime" type="gmtDateTime" minOccurs="0"/>
            </xsd:sequence>
            <xsd:attribute name="ReqId" type="quantity" use="required"/>
        </xsd:complexType>
    </xsd:element>
```

```
    <xsd:element name="LOGOFF">
        <xsd:annotation>
            <xsd:documentation>
=================================== LOGOFF ================================
Vendor Logoff message
===========================================================================

            </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType/>
    </xsd:element>
    <xsd:element name="CHNGPWDREQ">
        <xsd:annotation>
            <xsd:documentation>
================================ CHNGPWDREQ ===============================
Vendor change password command message
===========================================================================

            </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType>
            <xsd:sequence>
                <xsd:element name="Password">
                    <xsd:complexType>
                        <xsd:sequence>
                            <xsd:element name="Encoding">
                                <xsd:complexType>
                                    <xsd:group ref="SingleEncodedData"/>
                                    <xsd:attribute name="Notation" type="xsd:string" use="required"/>
                                </xsd:complexType>
                            </xsd:element>
                        </xsd:sequence>
                    </xsd:complexType>
                </xsd:element>
                <xsd:element name="NewPassword">
                    <xsd:complexType>
                        <xsd:sequence>
                            <xsd:element name="Encoding">
                                <xsd:complexType>
                                    <xsd:group ref="SingleEncodedData"/>
                                    <xsd:attribute name="Notation" type="xsd:string" use="required"/>
                                </xsd:complexType>
                            </xsd:element>
                        </xsd:sequence>
                    </xsd:complexType>
                </xsd:element>
            </xsd:sequence>
            <xsd:attribute name="ReqId" type="quantity" use="required"/>
        </xsd:complexType>
    </xsd:element>
    <xsd:element name="CHNGPWDRESP">
        <xsd:annotation>
            <xsd:documentation>
============================== CHNGPWDRESP ================================
Vendor change password command response
===========================================================================

            </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType>
            <xsd:sequence>
                <xsd:element ref="Status"/>
            </xsd:sequence>
            <xsd:attribute name="ReqId" type="quantity" use="required"/>
        </xsd:complexType>
    </xsd:element>
    <xsd:element name="FULLRECVYREQ">
        <xsd:annotation>
            <xsd:documentation>
================================ FULLRECVYREQ =============================
Full data recovery command message
===========================================================================

            </xsd:documentation>
```

```
        </xsd:annotation>
        <xsd:complexType>
            <xsd:attribute name="ReqId" type="quantity" use="required"/>
        </xsd:complexType>
    </xsd:element>
    <xsd:element name="PARTRECVYREQ">
        <xsd:annotation>

    <xsd:documentation>==================================PARTRECVYREQ==================
==============
Full data recovery command message
================================================================================
            </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType>
            <xsd:sequence>
                <xsd:element name="NewsSeqNo" type="long"/>
            </xsd:sequence>
            <xsd:attribute name="ReqId" type="quantity" use="required"/>
        </xsd:complexType>
    </xsd:element>
    <xsd:element name="RECVYRESP">
        <xsd:annotation>
            <xsd:documentation>
================================== RECVYRESP ==================================
Vendor change password command response
================================================================================
            </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType>
            <xsd:sequence>
                <xsd:element ref="Status"/>
                <xsd:element name="NoofNewsItem" type="quantity" minOccurs="0"/>
            </xsd:sequence>
            <xsd:attribute name="ReqId" type="quantity" use="required"/>
        </xsd:complexType>
    </xsd:element>
    <xsd:element name="RECVYCOMPLETE">
        <xsd:annotation>
            <xsd:documentation>
================================== RECVYCOMPLETE ==============================
New Recovery completed message
================================================================================
            </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType>
            <xsd:attribute name="ReqId" type="quantity" use="required"/>
        </xsd:complexType>
    </xsd:element>
    <xsd:element name="PERMISSIONDROP">
        <xsd:annotation>
            <xsd:documentation>
============================== PERMISSIONDROP ================================
Permission drop message
================================================================================
            </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType>
            <xsd:sequence>
                <xsd:element name="Reason" type="xsd:string"/>
            </xsd:sequence>
        </xsd:complexType>
    </xsd:element>
    <xsd:element name="UPDATEHEADLINE">
        <xsd:annotation>
            <xsd:documentation>
============================== UPDATEHEADLINE ================================
Headline update message
================================================================================
            </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType>
```

```
            <xsd:sequence>
                <xsd:element ref="NewsML"/>
            </xsd:sequence>
            <xsd:attribute name="Type" use="required">
                <xsd:simpleType>
                    <xsd:restriction base="xsd:string">
                        <xsd:enumeration value="ALERT"/>
                        <xsd:enumeration value="FIRSTTAKE"/>
                        <xsd:enumeration value="CANCELLED"/>
                        <xsd:enumeration value="AMENDED"/>
                    </xsd:restriction>
                </xsd:simpleType>
            </xsd:attribute>
            <xsd:attribute name="SeqNo" type="xsd:integer" use="required"/>
        </xsd:complexType>
    </xsd:element>
    <xsd:element name="RECVYHEADLINE">
        <xsd:annotation>
            <xsd:documentation>
============================== RECVYHEADLINE ==================================
Headline update message (Recovery)
================================================================================
            </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType>
            <xsd:sequence>
                <xsd:element ref="NewsML"/>
            </xsd:sequence>
            <xsd:attribute name="Type" use="required">
                <xsd:simpleType>
                    <xsd:restriction base="xsd:string">
                        <xsd:enumeration value="ALERT"/>
                        <xsd:enumeration value="FIRSTTAKE"/>
                        <xsd:enumeration value="CANCELLED"/>
                        <xsd:enumeration value="AMENDED"/>
                    </xsd:restriction>
                </xsd:simpleType>
            </xsd:attribute>
            <xsd:attribute name="SeqNo" type="xsd:integer" use="required"/>
        </xsd:complexType>
    </xsd:element>
    <xsd:element name="STATUSREQ">
        <xsd:annotation>
            <xsd:documentation>
================================== STATUSREQ ==================================
communication status request
================================================================================
        </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType>
            <xsd:attribute name="ReqId" type="quantity" use="required"/>
        </xsd:complexType>
    </xsd:element>
    <xsd:element name="STATUSRESP">
        <xsd:annotation>
            <xsd:documentation>
================================== STATUSRESP =================================
communication status request response
================================================================================
        </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType>
            <xsd:attribute name="ReqId" type="quantity" use="required"/>
        </xsd:complexType>
    </xsd:element>
    <xsd:element name="INITREQ">
        <xsd:annotation>
            <xsd:documentation>
================================== INITREQ ====================================
communication status request response
================================================================================
        </xsd:documentation>
```

```
        </xsd:annotation>
        <xsd:complexType>
            <xsd:attribute name="ReqId" type="quantity" use="required"/>
        </xsd:complexType>
    </xsd:element>
    <xsd:element name="INITRESP">
        <xsd:annotation>
            <xsd:documentation>
================================== INITRESP ====================================
Initialization response
================================================================================
        </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType>
            <xsd:sequence>
                <xsd:element ref="Status"/>
                <xsd:element name="SessionKey" minOccurs="0">
                    <xsd:complexType>
                        <xsd:sequence>
                            <xsd:element name="Encoding">
                                <xsd:complexType>
                                    <xsd:group ref="SingleEncodedData"/>
                                    <xsd:attribute name="Notation" type="xsd:string" use="required"/>
                                </xsd:complexType>
                            </xsd:element>
                        </xsd:sequence>
                    </xsd:complexType>
                </xsd:element>
            </xsd:sequence>
            <xsd:attribute name="ReqId" type="quantity" use="required"/>
        </xsd:complexType>
    </xsd:element>
    <xsd:element name="NDSML">
        <xsd:annotation>
            <xsd:documentation>
================================== NDSML ====================================
NDSML
================================================================================
        </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType>
            <xsd:sequence>
                <xsd:element ref="MsgHeader"/>
                <xsd:choice>
                    <xsd:element ref="INITREQ"/>
                    <xsd:element ref="INITRESP"/>
                    <xsd:element ref="LOGONREQ"/>
                    <xsd:element ref="LOGONRESP"/>
                    <xsd:element ref="LOGOFF"/>
                    <xsd:element ref="CHNGPWDREQ"/>
                    <xsd:element ref="CHNGPWDRESP"/>
                    <xsd:element ref="FULLRECVYREQ"/>
                    <xsd:element ref="PARTRECVYREQ"/>
                    <xsd:element ref="RECVYRESP"/>
                    <xsd:element ref="RECVYCOMPLETE"/>
                    <xsd:element ref="PERMISSIONDROP"/>
                    <xsd:element ref="STATUSREQ"/>
                    <xsd:element ref="STATUSRESP"/>
                    <xsd:element ref="UPDATEHEADLINE"/>
                    <xsd:element ref="RECVYHEADLINE"/>

                </xsd:choice>
            </xsd:sequence>
        </xsd:complexType>
    </xsd:element>
</xsd:schema>
```

Appendix B Base64 Encoding and Decoding Algorithms

Base 64 encoding is defined in RFC 1521. The basic concept is described in the following.

The first 6 bits (bits 1-6) are read and then those 6 bits are mapped to 8 bits that correspond to visible ASCII characters. The next 6 bits (bits 7-12) are read and these are mapped to 8 bits using the same mapping procedure. The same mechanism is applied for the next 6 bits (bits 13-18) and again for the next 6 bits (bits 19-24). Once 4 sets of 6 bits (24 bits total) are read, another byte boundary is encountered.

The translation table is as follows:

Input	Output	Input	Output	Input	Output	Input	Output
000000	A	010000	Q	100000	g	110000	w
000001	B	010001	R	100001	h	110001	x
000010	C	010010	S	100010	I	110010	y
000011	D	010011	T	100011	j	110011	z
000100	E	010100	U	100100	k	110100	0
000101	F	010101	V	100101	l	110101	1
000110	G	010110	W	100110	m	110110	2
000111	H	010111	X	100111	n	110111	3
001000	I	011000	Y	101000	o	111000	4
001001	J	011001	Z	101001	p	111001	5
001010	K	011010	a	101010	q	111010	6
001011	L	011011	b	101011	r	111011	7
001100	M	011100	c	101100	s	111100	8
001101	N	011101	d	101101	t	111101	9
001110	O	011110	e	101110	u	111110	+
001111	P	011111	f	101111	v	111111	/
(pad)	=						

When decoding, white space should be ignored. A '=' represents that the encoded file has been padded. If the input file contains a character that is not listed in the table above, is not white space, and is not a '=', then there is an error.

For encoding used in IIS, three bytes of data are read from the input file and then they are encoded as four bytes. When the input file is not a multiple of 3 bytes in length, the following handlings should be followed.

1. If the input file is a multiple of 3 bytes in length.
Then there is no problem. The last read from the file will be three bytes in length.
First encoded byte: 1-6 bits of the input
Second encoded byte: 7-12 bits of the input
Third encoded byte: 13-18 bits of the input
Fourth encoded byte: 19-24 bits of the input

2. If the input file is a multiple of 3 bytes in length plus one.
The last read from the file will be one byte (8 bits) in length.
First encoded byte: 1-6 bits of the input byte
Second encoded byte: 7-8 bits of the input byte + "0000"
Third encoded byte: '='
Fourth encoded byte: '='

3. If the input file is a multiple of 3 bytes in length plus two.
The last read from the file will be two bytes (16 bits) in length.
First encoded byte: 1-6 bits of the input byte
Second encoded byte: 7-12 bits of the input
Third encoded byte: 13-16 bits of the input + "00"
Fourth encoded byte: '='

Appendix C Cryptography in IIS

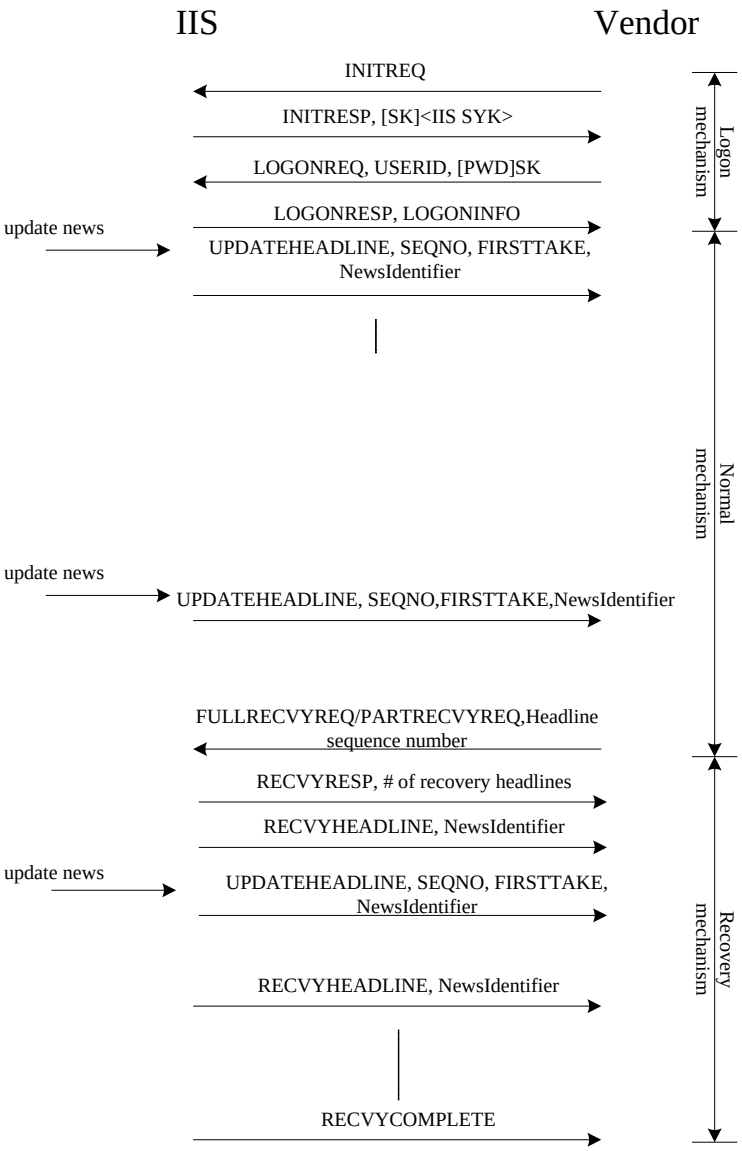
ENCRYPTION AND DECRYPTION ALGORITHMS

The encryption and decryption algorithms being used in IIS are Triple-DES algorithm in Microsoft CryptoAPI with Triple DES - Cyclic Block Chaining mode (3DES-CBC), and PKCS5 Padding.
Please refer to the Microsoft Web Site for detailed information of the Microsoft CryptoAPI.
<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/seccrypto/security/cryptography_portal.asp>
For password processing, the Vendor terminal receives INITRESP message with session key which is encrypted by IIS symmetric key. The IIS symmetric key is distributed by the Exchange to each Vendor. Having got session key, the Vendor terminal sends encrypted password using session key in LOGONREQ message. The same mechanism is used for CHNGPWDREQ message for change of password.

The procedure to obtain plain text session key in INITREQ message is as follows.
1. Decode session key value using Base64 algorithm
2. Decrypt session key value using PK3
3. Encrypt session key value using PK2
4. Decrypt session key value using PK1

The procedure to create encrypted password in LOGONREQ and CHNGPWDREQ messages is in the following.
1. Encrypt password using PK1
2. Decrypt password using PK2
3. Encrypt password using plain text session key value obtained in the above steps

Appendix D An example of Message Flow Diagram



Appendix E Error Code Definition

Error	Error code	Error Message
INVALID_MESSAGE	90001	Invalid message format
PERMISSION_DROP	90002	Permission is revoked.
SESSION_NOT_ESTABLISHED	90004	Vendor haven't sign on
SERVICE_NOT_ALLOW	90005	No permission to request the service.
DUPLICATE_LOGON	90006	Vendor session had been established.
NEWS_NOT_FOUND	90007	No such headline or headline has been housekept
INCORRECT_VENDOR	90010	Incorrect Vendor identity or password
SERVICE_NOT_AVAILABLE	90012	Service is not available
INVALID_PASSWORD	90013	Invalid Password
SYSTEM BUSY	90014	System Busy

Appendix F Subject Code and Scheme within DescriptiveMetadata

There are different kinds of subject code comes within DescriptiveMetadata which is identified by the scheme name. Scheme can be headlinecategory, stock code, stock name, market code, expiry date, etc. The following table summarizes the possible types of scheme within subject code.

Scheme	Description
Stock Code	Stock Code of the stock related to the news
Stock Name	Stock Name of the stock related to the news Notes: ▪ In NewsML, the Stock Name will be encoded in Base64 format ▪ For trading news, the stock name field will be empty
Expiry Date	Expiry Date of the news
Headline Category – T1	Code of the News Category representing the Tier 1 announcement headlines – the most representative news category input by the listed issuer Notes: ▪ For trading news and nasdaq, the Headline Category – T1 field will be empty
Headline Category – T2	Code of the announcement Category Code for the Tier 2 headlines in order of their importance. Tier 2 News Categories are other news category also covered by the News input by the listed issuer.
Mkt Code	Market Code of the news

The following table summarizes the possible Market Code of the subject code with scheme **Mkt Code**. The maximum description length for Headline Category is 200 bytes.

Market Code (Scheme=Mkt Code)

Market Code	Description
ALL	All markets
MAIN	Main Board
GEM	GEM Board
NASD	Nasdaq securities
ETS	Extended Trade Securities including “iShares” that is traded during lunch time

Expiry Date (Scheme=Expiry Date)

Format	Description
CCYYMMDD	Current News Expiry Date

Trading News Headline Category (Scheme=Headline Category-T2)*

Tier 2 Headline Category	Chinese Description	Description
EXN	交易所訊息	Trading News issued by the Exchange

* Notes for Trading News Headline Category:

- The news will come with empty Tier 1 Headline Category. All associated Headline Category will be delivered as Tier 2 Headline Category.
- Tier 2 Headline Categories under Trading News Headline Category do not belong to the Headline Categories defined in the Listing Rules for issuer announcements.

Main Broad and GEM Broad Headline Category (defined in the Listing Rules)

* T1 – Tier 1 Headline Category Code (Scheme=Headline Category-T1)
**T2 – Tier 2 Headline Category Code (Scheme=Headline Category-T2)

T1*	T2**	Description	Chinese Description
10000		Announcements and Notices	公告及通告
		Connected Transactions	關連交易
	11100	Auditors or INEDs Unable to Confirm Matters relating to Continuing Connected Transaction	核數師或獨立非執行董事未能確認有關持續關連交易的事宜
	11200	Connected Transaction	關連交易
	11300	Continuing Connected Transaction	持續關連交易
	11400	Guaranteed Net Tangible Assets or Profits	擔保有形資產淨值或溢利
	11500	Waiver in respect of Connected Transaction Requirements	就關連交易規定所授予的豁免
		Corporate Positions and Committees/Corporate Changes	公司狀況變動及委員會／公司變動
	12100	Amendment of Constitutional Documents	修訂憲章文件
	12150	Change in Auditors	更換核數師
	12200	Change in Class Rights	更改不同類別股份的權利
	12250	Change in Compliance Adviser	更換合規顧問
	12300	Change in Compliance Officer	更換監察主任
	12350	Change in Directors or of Important Executive Functions or Resposnibilities	更換董事或重要行政職能或職責的變更
	12400	Change in Financial Year End	更改財政年度結算日期
	* 12450	Change in Qualified Accountant	更換合資格會計師
	12500	Change in Registered Address or Office, Registered Place of Business in HK or Agent for Service of Process in HK	更改註冊地址或辦事處、香港業務的註冊地或香港接收法律程序文件代表
	12550	Change in Company Secretary	更換公司秘書
	12600	Change in Supervisors	更換監事

	12650	Change of Audit Committee Member	更換審核委員會成員
	12700	Change of Company Name	更改公司名稱
	12750	Non-compliance with Audit Committee Requirements	未能符合審核委員會的規定
	12800	Non-compliance with Compliance Officer Requirements	未能符合監察主任的規定
	12850	Non-compliance with INED Requirements or INED Failing to Meet Independence Guidelines	未能符合獨立非執行董事的規定或獨立非執行董事未能符合獨立性指引
	* 12900	Non-compliance with Qualified Accountant Requirements	未能符合合資格會計師的規定
	12950	Change in a Director's or Supervisor's Biographical Details	董事或監事履歷詳情的變更
	12951	Change in Chief Executive	更換行政總裁
	12952	List of Directors and their Role and Function	董事名單和他們的地位和作用
	12953	Non-compliance with Remuneration Committee Requirements	未能符合薪酬委員會的規定
	12954	Terms of Reference of the Audit Committee	審核委員會的職權範圍
	12955	Terms of Reference of the Nomination Committee	提名委員會的職權範圍
	12956	Terms of Reference of the Remuneration Committee	薪酬委員會的職權範圍
	12957	Change of Remuneration Committee Member	更換薪酬委員會成員
	12958	Terms of Reference of Other Board Committees	其他董事會轄下之委員會的職權範圍
		Financial Information	財務資料
	13100	Advance to an Entity	向實體提供墊款
	13150	Date of Board Meeting	董事會召開日期
	13200	Delay in Results Announcement	延遲發表業績公告
	13250	Dividend or Distribution	股息或分派
	13300	Final Results	末期業績
	13350	Financial Assistance and/or Guarantee to Affiliated Company	向聯屬公司提供財務資助及／或作出擔保
	13400	Interim Results	中期業績

	13450	Net Asset Value	資產淨值
	13500	Profit Warning	盈利警告
	13550	Qualified and/or Modified Audit Report	附帶「保留意見」及／或「修訂意見」的核數師報告
	13600	Quarterly Results	季度業績
	13650	Results of a Subsidiary	附屬公司的業績
	13700	Revision of Information in Published Preliminary Results	修訂已刊發初步業績的資料
		Meetings/Voting	會議／表決
	14100	Change of Voting Intention	更改表決意向
	14200	Material Information after Issue of Circular	在發出通函後的重大資料
	14300	Nomination of Director by Shareholder	由股東提名董事
	14400	Notice of AGM	股東周年大會通告
	14500	Notice of EGM/SGM	股東特別大會通告
	14600	Re-election or Appointment of Director subject to Shareholders' Approval	在股東批准的情況下重選或委任董事
	14700	Results of AGM	股東周年大會的結果
	14800	Results of EGM/SGM	股東特別大會的結果
	* 14900	Results of Voting by Poll	投票表決的結果
	15000	Change in Auditors subject to Shareholders' Approval	在股東批准的情況下更換核數師
		New Listings (Listed Issuers/New Applicants)	新上市（上市發行人／新申請人）
	15100	Allotment Results	配發結果
	15200	Formal Notice	正式通告
	15300	Listing of Securities by way of Introduction	以介紹形式上市的證券
	15400	Striking Price on Offer for Subscription or for Sale by Tender	供認購或投標發售的行使價
	15500	Supplemental Information regarding IPO	有關首次公開招股的補充資料
	15600	Transfer of listing from GEM to Main Board	由創業板轉往主板上市

	15700	Mixed Media Offer	混合媒體要約
		Notifiable Transactions	須予公布的交易
	16100	Delay in Completion	在完成須予公布的交易方面出現延誤
	16200	Discloseable Transaction	須予披露的交易
	16300	Major Transaction	主要交易
	16400	Reverse Takeover	反收購
	16500	Share Transaction	股份交易
	16600	Termination of Transaction	終止交易
	16700	Variation to Terms	條款上的更改
	16800	Very Substantial Acquisition	非常重大的收購事項
	16900	Very Substantial Disposal	非常重大的出售事項
		Reorganisation/Change in Shareholding/Major Changes/Public Float/Listing Status	重組／股權變動／主要改動／公眾持股量／上市地位
	17100	Announcement by Offeree Company under theTakeovers Code	《收購守則》所指的受要約公司刊發的公告
	17150	Announcement by Offeror Company under theTakeovers Code	《收購守則》所指的要約公司刊發的公告
	17200	Change in Shareholding	股權出現變動
	17250	Charging or Pledging of Shares by Shareholder	股東抵押股份
	17300	Concentration of Shareholdings	股權集中
	17350	Dealing in Securities by Director where Otherwise Prohibited under Model Code	董事於《標準守則》所載的禁售期內買賣證券
	* 17400	Fundamental Change in Principal Business Activities	主要業務活動出現根本轉變
	17450	Group Restructuring or Scheme of Arrangement	集團重組或協議安排
	17500	Lack of Open Market in Securities	證券缺乏公開市場
	17550	Listing on Overseas Exchange or Securities Market	於海外交易所或證券市場上市
	17600	Privatisation/Withdrawal or Cancellation of Listing of	私有化／撤銷或取消證券上市

		Securities	
	17650	Resumption	復牌
	17700	Spin-off	分拆
	17750	Sufficiency of Assets and/or Operations and/or Issuer becoming Cash Company	資產充足度及／或業務充足度及／或發行人成為現金資產公司
	17800	Sufficiency of Public Float	公眾持股量充足度
	17850	Suspension	停牌
	17900	Winding Up and Liquidation of Issuer, its Holding Company or Major Subsidiary	發行人、其控股公司或主要附屬公司結束營業及清盤
	17950	Change in Principal Business Activities	主要業務活動出現轉變
	17960	Trading Halt	短暫停牌
		Securities/Share Capital	證券／股本
	18100	Announcement pursuant to Code on Share Repurchases	根據《股份購回守則》發出的公告
	18120	Capital Reorganisation	資本重組
	18140	Capitalisation Issue	資本化發行
	18160	Change in Board Lot Size	更改每手買賣單位
	18180	Change in Terms of Securities or Rights attaching to Securities	更改證券條款或隨附於證券的權利
	18200	Change of Dividend Payment Date	更改股息支付日期
	18220	Closure of Books or Change of Book Closure Period	暫停辦理過戶登記手續或更改暫停辦理過戶日期
	18240	Consideration Issue	代價發行
	18260	Conversion of Securities	轉換證券
	18280	Intention to Sell Shares of Untraceable Member	出售未能聯絡到的股東股份的意向
	18300	Issue of Convertible Securities	發行可轉換證券
	18320	Issue of Debt Securities	發行債務證券
	18340	Issue of Preference Shares	發行優先股

	18360	Issue of Securities by Major Subsidiary	主要附屬公司發行證券
	18380	Issue of Shares under a General Mandate	根據一般性授權發行股份
	18400	Issue of Shares under a Specific Mandate	根據特定授權發行股份
	18420	Issue of Warrants	發行權證
	18440	Movements in Issued Share Capital	已發行股本變動
	18460	Open Offer	公開招股
	18480	Placing	配售
	18500	Rights Issue	供股
	18520	Share Option Scheme	股份期權計劃
	18540	Trading Arrangements (other than Change in Board Lot Size)	交易安排（更改每手買賣單位除外）
		Miscellaneous	雜項
	19100	Breach of Loan Agreement	違反借貸協議
	19150	Clarification of News or Reports – Qualified	澄清新聞報道或報告 – 附帶意見
	19200	Clarification of News or Reports – Standard or Super	澄清新聞報道或報告 – 標準內容或超級內容
	19250	Delay in Dispatch of Circular or other Document	延遲發送通函或其他文件
	19300	Loan Agreement with Specific Performance Covenant	附有特定履行契諾的借貸協議
	19350	Matters relating to Options	有關期權事宜
	19400	Matters relating to Collective Investment Schemes	有關集體投資計劃事宜
	19450	Other	其他
	19500	Overseas Regulatory Announcement	海外監管公告
	** 19550	Price-Sensitive Information	股價敏感資料
	19600	Unusual Price/Turnover Movements – Qualified	不尋常價格／成交量變動 – 附帶意見
	19650	Unusual Price/Turnover Movements – Standard or Super	不尋常價格／成交量變動 – 標準內容或超級內容
	19700	Mining Activities Undertaken by Listed Issuers	上市發行人所從事的礦業活動

	19750	Inside Information	內幕消息
20000		Circulars	通函
		Connected Transaction	關連交易
	21100	Connected Transaction	關連交易
	21200	Continuing Connected Transaction	持續關連交易
		Corporate Positions and Committees/Corporate Changes	公司狀況變動及委員會／公司變動
	22100	Amendment of Constitutional Documents	修訂憲章文件
		Meetings/Voting	會議／表決
	23100	Change of Voting Intention	更改表決意向
	23200	Material Information after Issue of Circular	發出通函後的重大資料
	23300	Nomination of Director by Shareholder	由股東提名董事
	23400	Re-election or Appointment of Director subject to Shareholders' Approval	在股東批准的情況下重選或委任董事
	23500	Change in Auditors subject to Shareholders' Approval	在股東批准的情況下更換核數師
		Notifiable Transactions	須予公布的交易
	* 24100	Discloseable Transaction	須予披露的交易
	24200	Major Transaction	主要交易
	24300	Reverse Takeover	反收購
	24400	Very Substantial Acquisition	非常重大的收購事項
	24500	Very Substantial Disposal	非常重大的出售事項
		Reorganisation/Change in Shareholding/Major Changes/Public Float/Listing Status	重組／股權改動／主要改動／公眾持股量／上市地位
	25100	Document issued by Offeree Company under the Takeovers Code	《收購守則》所指的受要約公司發出的文件
	25200	Document issued by Offeror Company under the Takeovers Code	《收購守則》所指的要約公司發出的文件
	25300	Fundamental Change in Principal Business Activities	主要業務活動出現根本轉變

	25400	Privatisation/Withdrawal of Listing of Securities	私有化／撤銷證券上市
	25500	Proposal of Mineral Company to Explore for Natural Resources as Extension to or Change from Existing Activities	有關礦務公司開發天然資源用以拓展或更改現有活動的建議
	25600	Spin-off	分拆
		Securities/Share Capital	證券／股本
	26100	Capitalisation Issue	資本化發行
	26150	Change in Terms of Securities or Rights attaching to Securities	更改證券條款或隨附於證券的權利
	26200	Document issued pursuant to Code on Share Repurchases	根據《股份購回守則》刊發的文件
	26250	Exchange or Substitution of Securities	交換證券或取代原證券
	26300	Explanatory Statement for Repurchase of Shares	回購股份的說明函件
	26350	General Mandate	一般性授權
	26400	Issue of Convertible Securities	發行可轉換證券
	26450	Issue of Debt Securities	發行債務證券
	26500	Issue of Preference Shares	發行優先股
	26550	Issue of Securities by Major Subsidiary	主要附屬公司發行股份
	26600	Issue of Securities within 6 Months of Listing	於上市後六個月內發行證券
	26650	Issue of Shares	發行股份
	26700	Issue of Warrants	發行權證
	26750	Open Offer	公開招股
	26800	Rights Issue	供股
	26850	Share Option Scheme	購股權計劃
		Miscellaneous	雜項
	27100	Matters relating to Collective Investment Schemes	有關集體投資計劃事宜
	27900	Other	其他

30000		Listing Documents	上市文件
	30100	Authorised Collective Investment Scheme	認可集體投資計劃
	30200	Capitalisation Issue	資本化發行
	30300	Deemed New Listing under the Listing Rules	按《上市規則》規定視為新上市
	30400	Exchange or Substitution of Securities	交換證券或取代原證券
	30500	Introduction	介紹
	30600	Offer for Sale	發售現有證券
	30700	Offer for Subscription	發售以供認購
	30800	Open Offer	公開招股
	30900	Other	其他
	31000	Placing of Securities of a Class New to Listing	配售上市後的新證券類別
	31100	Rights Issue	供股
	31200	Supplementary Listing Document	補充上市文件
40000		Financial Statements/ESG Information	財務報表/環境、社會及管治資料
	40100	Annual Report	年報
	40200	Interim/Half-Year Report	中期／半年度報告
	40300	Quarterly Report	季度報告
	40400	Environmental, Social and Governance Information/Report	環境、社會及管治資料/報告
70000		Debt and Structured Products	債券及結構性產品
		Trading Summaries - Derivative Warrants	交易摘要－衍生權證
	71100	Daily Trading Report on Derivative Warrant	衍生權證每日交易報告
	71200	Pre-Listing Trading Report on Derivative Warrant	衍生權證上市前的交易報告
		Trading Summaries - Equity Linked Instruments	交易摘要－股票掛鈎票據
	71300	Daily Trading Report on Equity Linked Instrument	股票掛鈎票據每日交易報告
	71400	Pre-Listing Trading Report on Equity Linked Instrument	股票掛鈎票據上市前的交易報告

		Trading Summaries - Callable Bull/Bear Contracts	交易摘要－牛熊證
	71500	Daily Trading Report on Callable Bull/Bear Contract	牛熊證每日交易報告
	71600	Pre-Listing Trading Report on Callable Bull/Bear Contract	牛熊證上市前的交易報告
		Warrant Announcements - Derivative Warrants	權證公告－衍生權證
	72100	Announcement regarding Exotic Derivative Warrant	有關非標準型衍生權證的公告
	72150	Expiry Announcement regarding Derivative Warrant	衍生權證到期公告
	72200	Launch Announcement regarding Derivative Warrant	衍生權證發行公告
	72250	Other Announcement regarding Derivative Warrant	有關衍生權證的其他公告
		Warrant Announcements - Equity Linked Instruments	權證公告－股票掛鈎票據
	72300	Announcement regarding Exotic Equity Linked Instrument	有關非標準型股票掛鈎票據的公告
	72350	Expiry Announcement regarding Equity Linked Instrument	股票掛鈎票據到期公告
	72400	Launch Announcement regarding Equity Linked Instrument	股票掛鈎票據發行公告
	72450	Other Announcement regarding Equity Linked Instrument	有關股票掛鈎票據的其他公告
		Warrant Announcements - Callable Bull/Bear Contracts	權證公告－牛熊證
	72500	Announcement regarding Exotic Callable Bull/Bear Contract	有關非標準型牛熊證的公告
	72550	Expiry Announcement regarding Callable Bull/Bear Contract	牛熊證到期公告
	72600	Launch Announcement regarding Callable Bull/Bear Contract	牛熊證發行公告
	72650	Other Announcement regarding Callable Bull/Bear Contract	有關牛熊證的其他公告
		Warrant Listing Documents – Derivative Warrants	權證上市文件－衍生權證
	73100	Base Listing Document of Derivative Warrant	衍生權證的基礎上市文件
	73200	Supplemental Listing Document of Derivative Warrant	衍生權證的補充上市文件
		Warrant Listing Documents – Equity Linked Instruments	權證上市文件－股票掛鈎票據

	73300	Base Listing Document of Equity Linked Instrument	股票掛鈎票據的基礎上市文件
	73400	Supplemental Listing Document of Equity Linked Instrument	股票掛鈎票據的補充上市文件
		Warrant Listing Documents – Callable Bull/Bear Contracts	權證上市文件－牛熊證
	73500	Base Listing Document of Callable Bull/Bear Contract	牛熊證的基礎上市文件
	73600	Supplemental Listing Document of Callable Bull/Bear Contract	牛熊證的補充上市文件
		Debt Securities Announcements	債務證券公告
	74100	Formal Notice	正式通告
	74200	Other Announcement regarding Debt Securities	有關債務證券的其他公告
	74300	Overseas Regulatory Announcement	海外監管公告
		Others	其他
	75100	Debt Securities Offering Circular and Pricing Supplement	債務證券發行通函或定價補充文件
	75200	Debt Securities Prospectus	債務證券招股章程
	75300	Issuer-Specific Report	發行人－指定報告
52000		Proxy Forms	委任代表表格
90000		Regulatory Announcement & News	監管者發出的公告及消息
80000		Trading Information of Exchange Traded Funds	交易所買賣基金的交易資料
50000		Next Day Disclosure Returns	翌日披露報表
	50100	Share Buyback	股份購回
	50200	Others	其他
* 51000		Share Buyback Reports	股份購回報告
51500		Monthly Returns	月報表
53000		Company Information Sheet (GEM)	公司資料報表（「創業板」）

54000		Constitutional Documents	憲章文件
55000		Takeovers Code – dealing disclosures	合併守則- 交易披露
MISC	MISC	Miscellaneous	雜項

*** Headline ceased to be used since 1 January 2009**
**** Headline ceased to be used since 1 January 2013**
The code "MISC" under both Tier 1 and Tier 2 headline category does not belong to Headline Categories of issuer announcements defined in the Listing Rules.

Below is the example that illustrates the structure of <Descriptive Metadata> tag:

```
<DescriptiveMetadata>
        <Language FormalName=”[X]*” />
        <SubjectCode>



                <!-- Announcement Category (Tier 1) of the news -->
                <SubjectMatter FormalName=”11000” Scheme=”Headline Category-T1”/>

                <!-- Announcement Category (Tier 2) of the news -->
                <SubjectMatter FormalName=”13000” Scheme=”Headline Category-T2”/>
                <SubjectMatter FormalName=”12000” Scheme=”Headline Category-T2”/>
                <SubjectMatter FormalName=”14000” Scheme=”Headline Category-T2”/>


                <!-- Market Code of the news -->
                <SubjectMatter FormalName=”MAIN” Scheme=”Mkt Code”/>

                <!-- Expiry Date of the news -->
                <SubjectMatter FormalName=”20031203” Scheme=”Expiry Date”/>

                <!-- Stock Information for first stock related to this news -->
                <SubjectMatter FormalName="00013” Scheme=”Stock Code”/>
                <SubjectMatter FormalName="STOCK NAME FOR 00013” Scheme=”Stock Name”/>

                <SubjectMatter FormalName="00383” Scheme=”Stock Code”/>
                <SubjectMatter FormalName="STOCK NAME FOR 00383” Scheme=”Stock Name”/>

        </SubjectCode>
</DescriptiveMetadata>
```