Annex 3

HELCOM RECOMMENDATION 33/1

Adopted 6 March 2012
having regard to Article 20, Paragraph 1 b)
of the Helsinki Convention

UNIFIED INTERPRETATION IN RELATION TO ACCESS TO AND USE OF HELCOM AIS

THE COMMISSION,

RECALLING the HELCOM Extraordinary Ministerial Meeting in Copenhagen on 10 September 2001 which decided to establish a Working Group with the purpose of facilitating mutual exchange and deliveries of AIS-data, including the construction of the monitoring system for the maritime traffic in the Baltic Sea Area,

RECALLING FURTHER Regulation 9 of Annex IV to the Helsinki Convention on the use of Automatic Identification System,

ACKNOWLEDGING the successful establishment of the HELCOM Automatic Identification System as regulated by the HELCOM Agreement on Access to AIS Information, and its contribution to the improved safety of navigation and protection of the marine environment in the Baltic Sea area,

APPRECIATING the cooperation among the Baltic Sea countries as well as Norway in maintaining and further developing the HELCOM AIS, taking place within the HELCOM Expert Working Group for Mutual Exchange and Deliveries of AIS data,

HAVING IN MIND the HELCOM Baltic Sea Action Plan, adopted by the HELCOM Ministerial Meeting on 15 November 2007, and the agreement included therein to amend the HELCOM Agreement on Access to AIS Information by 2008 taking into account the proposal elaborated by the 16th Meeting of the HELCOM Expert Working Group for Mutual Exchange and Deliveries of AIS data (HELCOM AIS EWG 16/2007),

OBSERVING the growing interest to use HELCOM AIS data, both within the Baltic Sea countries and Norway as well as in other geographical regions,

RECOGNIZING the need for common interpretation regarding the use of and access to HELCOM AIS, in light of new services that have been made available to the AIS users, including web based historical data extract, web based real-time AIS display and real-time AIS data exchange,

RECOMMENDS the Governments of the Contracting States as well as Norway to apply the attached Guidelines on unified interpretation in relation to access to and use of HELCOM AIS,

REQUESTS the AIS Expert Working Group to regularly evaluate the implementation of this Recommendation and amend the attached Guidelines as need be.

Guidelines on unified interpretation in relation to access to and use of HELCOM AIS

Definitions

The definitions used by IALA and IMO are used in this document.

Objective

This Recommendation provides for exchange of AIS-data free of charge between the countries in accordance with the HELCOM Copenhagen Declaration adopted on 10 September 2001 in Copenhagen. It also provides for the distribution and use of the AIS-data received from the Participating parties (HELCOM Contracting States and Norway) with a general aim of enhancing the maritime safety and protection of the Baltic Sea environment as provided for in the Helsinki Convention. Additionally, the Recommendation includes a procedure to deal with all other interests in use of these HELCOM AIS data.

Access to information

Each Participating party shall make AIS-data available for access according to the method decided by the AIS Expert Working Group via Internet as outlined in *Appendix 2*.

AIS-data from all SOLAS ships carrying AIS as mandatory equipment shall be made available. AIS-data for other domestic ships is recommended to filter so other countries do not see them. Ships involved in operations mentioned in *Appendix 1* should preferably not be filtered.

Distribution and use of *real-time, historical and statistical HELCOM* AIS data

Each Participating party must restrict the distribution of received HELCOM AIS-data to the users and uses as expressed in *Appendix 1*.

Each Participating party is responsible for the use of distributed HELCOM AIS-data and must take appropriate actions to ensure that the recipients do not redistribute HELCOM AIS-data and that HELCOM AIS-data are only used for purposes listed in *Appendix 1*.

Any Participating party may, however, distribute data to a third person in the event that the participating nation is obliged by law to disclose information according to principles of public access to official records.

In order to deal with interests in distribution and use of HELCOM AIS data beyond the uses and/or users stipulated in *Appendix 1*, the following procedure shall be applied:

1. The HELCOM Secretariat will act as a contact point for receiving applications for granting access to and use of HELCOM AIS data.

2. The Secretariat will verify the information contained in an application for access to HELCOM AIS data.

3. The Secretariat will dispatch via facsimile and e-mail the verified application to all Participating Parties represented by the Heads of Delegation to HELCOM and contact persons for HELCOM Agreement on Access to AIS Information and the Norwegian Coastal Administration.

4. The decision by the Heads of Delegation to HELCOM and the Norwegian Coastal Administration on granting access to HELCOM AIS data or refraining from doing so will be communicated to the HELCOM Secretariat in writing.

5. Access to HELCOM AIS data will be granted only if such access is approved by all the Participating Parties.

6. The Participating Parties should consider the application and communicate the decision made to the HELCOM Secretariat within 30 days after the dispatch of the request to the Participating Parties. The HELCOM Secretariat should inform the applicant about the decision made within a fortnight.

7. A standard agreement on the use of HELCOM AIS data, providing for possible restrictions in access to HELCOM AIS data, will be signed between the applicant and HELCOM. The standard agreement is provided in *Appendix 3*.

8. The Danish Maritime Authority will be informed about the decision by the Participating Parties in order to implement within a reasonable timeframe the required technical solution needed for submitting the requested HELCOM AIS data to the applicant.

Information concerning private persons

When AIS-data contain information concerning private persons the Participating parties undertake to ensure protection of the privacy of these persons in accordance with the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (for EU countries) and also to other international, European Community and national law and regulations as applicable.

No warranties

The transmitting or sending party makes no express or implied warranty as to any matter whatsoever, including the availability, accuracy, or reliability of any information or data, whether tangible or intangible, made, developed or supplied under this Recommendation, or the ownership, merchantability, or fitness for a particular purpose of the information, of the data made, developed or supplied.

Force Majeure

Neither Participating party shall be liable for any unforeseeable event beyond its reasonable control not caused by the fault or negligence of such party, which causes such party to be unable to perform its obligations under the Agreement on Access to AIS Information, including, but not limited to, flood, drought, earthquake, storm fire, pestilence, lightning and other natural catastrophes, epidemic, war, riot, civic disturbance or disobedience, strikes, labour dispute, or failure, threat or failure, or sabotage, or any order or injunction made by a court or public agency. In the event of the occurrence of such a Force Majeure event, the party unable to perform shall promptly notify the other party. It shall further use its best efforts to resume performance as quickly as possible and shall suspend performance only for such period of time as is necessary as a result of the Force Majeure event.

Contact persons

A list of names and contact details for contact persons will be kept and updated by the HELCOM Secretariat.

Termination of access to AIS-data

Any failure to comply with this Recommendation gives the sending or transmitting party right to terminate access to AIS-data for as long as the receiving party is not complying with the Recommendation.

APPLICATIONS FOR RETRIEVED AIS DATA FROM THE COMMON BALTIC SEA AIS

Real-time AIS data in this agreement is defined to be:
- delivered end-to-end non-stop, one vessel report after the other as soon as they are transmitted
- delivered promptly when they are received at the base station
- delivered without any delay (additional latency)
- not sent in blocks
- irrespective of the reporting interval (not all messages received by the national centre are relayed/forwarded to the regional centre. The reporting interval is less frequent)

Type of access:

For each specific case some restrictions – at the discretion of a Participating Party - can be applied, where applicable and justified, such as: time limitation, geographical limitation and/or update rate.

Whenever access is implemented directly from the HELCOM AIS Information Centre, it is given for all Participating Parties' data* and at the update rate in-force.

If an access to a full update rate is needed this should be solved on a bilateral basis.

Type of AIS data:
- Real time (R),
- Statistic data** (S),
- Historical data (H)
- Web based visualization of AIS real-time data** (V)

User	Uses	Type of AIS data
HELCOM Secretariat	Aiming at implementation of the Helsinki Convention	S, H, V
National administration, including accident investigation authorities and any research institutes or organizations or their contractors in the Baltic Sea states and Norway acting according to the uses set herein	- Pollution preventing and combating - VTS (Vessel Traffic Services) - Port State Control (PSC) - Contingency planning - International Ship and Port Security (ISPS) - Search and Rescue (SAR) - Accident investigation - Traffic planning, efficiency and management, incl. icebreaking services - Mandatory reporting system for HAZMAT reporting requirements - Pilotage - Customs surveillance - Science and research supporting the implementation of the Helsinki Convention and for preparing IMO ships routeing measures	R, S, H, V
EU institutions Institutions in Russia	Aiming at implementation of the Helsinki Convention, including: - Mandatory reporting system for HAZMAT reporting requirements - Traffic planning - Pollution prevention - Maritime safety and security	R, S, H, V

The table may require further consideration to define in detail information to be exchanged among Participating Parties.

_____

* Except for real-time streamed data that can be filtered on the basis of the countries' AIS data
** Currently limited to 5 accounts per country involved due to technological reasons

Appendix 2

HELCOM Server

Description of connection interface

Introduction

Purpose

This document describes the two interfaces relevant to the participating parties wanting to exchange live AIS data with the HELCOM server.

Scope

The document describes how to supply data, and how to subscribe to data, divided into two scenarios:

Scenario 1: Testing and preparation period (October 2004 – January 2005)

The purpose of the testing and preparation period is to facilitate 'hole-through' testing, where any technical difficulties regarding the process of supplying and subscribing are resolved, and operational experience regarding bandwidth usage etc. is gained.

The HELCOM Server will gather all AIS data supplied in the database, in order to enable testing of statistics features. The connection setup will be quite simple.

(Participating parties technical representative should contact an appointed person in the Danish Maritime Authority for agreement on a plan for testing and specific details on IP addresses and port numbers.)

Scenario 2: Beta-release period (February 2005 – May 2005)

After the Beta-release of the HELCOM server late January 2005, another connection setup including security measures will be implemented. A 'Client Proxy' application will be supplied to the participating parties, which can be executed locally, and the Client Proxy will from this point represent the connection interface to the HELCOM Server. Between the Client Proxy and the HELCOM Server, a logon mechanism and a SSL (Secure Socket Layer) connection will ensure security.

References

Reference Name	Comments
IEC 61162-1	Maritime Navigation and Radio communication Equipment and Systems Part 1: Single talker and single listeners", as revised 2001. Edition 2.0.
IEC/PAS 61162-100	Maritime Navigation and Radio communication Equipment and Systems – Digital interfaces - Part 101: Single talker and multiple listeners – Extra requirements to IEC 61162-1 for the UAIS Edition 1.0
IEC/PAS 61162-101	Maritime Navigation and Radio communication Equipment and Systems Part 101: Single talker and multiple listeners – Modified sentences and requirements for IEC 61162-1. Edition 1.0

Definitions, Acronyms, and Abbreviations

Definition Name	Comments
Subscriber Application	The AIS Client Proxy can be used with any software capable of understanding IEC 61162-1 format compliant AIS data. E.g. a database application storing data, a statistics program, or a chart application displaying the AIS information e.g. Adveto.
Client Proxy	The AIS Client Proxy is the program used to gain access to the HELCOM AIS data, as described in this document.
HELCOM_IP	IP address from which the HELCOM server will connect to the AIS data suppliers. TBD(1)
PROXY_MAN	Land based AIS Client Proxy User Manual.

Interface Description

This section describes the interface used when supplying data to and receiving data from the HELCOM server.

Data format

The data must adhere to the IEC 61162-1, IEC/PAS 61162-100 and IEC/PAS 61162-101 standards, i.e. AIS messages are wrapped in the VDM or VDO sentences, resembling the output on the Presentation Interface of a Base Station.

When supplying data to the HELCOM server the participating parties will supply a TCP/IP socket connection (i.e. like a telnet connection, defined by a fixed IP address and port number) where data from their AIS system is available.

Similarly, a TCP/IP socket connection will be available for retrieving data from the HELCOM Server.

Security

It has been decided that in the testing period, the only way data can be supplied to / received from the HELCOM server is trough a standard socket connection from specific IP addresses. After the Beta-release, SSL connections via the Client Proxy will be enforced.

The use of VPN (Virtual Private Network) has been abandoned, due to the difficulties involved in administering many different VPN connections, plus the fact that a VPN connection may grant VPN users access to more resources on the targeted network than intended, while the SSL connection is very specific and considered sufficiently secure.

Connection setup

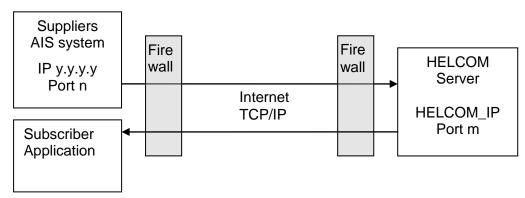**Scenario 1: Testing and preparation period (October 2004 – January 2005)**

Figure 1: HELCOM server retrieving data over a TCP/IP socket connection.

During the testing and preparation period, the HELCOM Server will connect directly to the suppliers AIS service and start collecting data, via a TCP/IP socket connection. The participating parties must supply the HELCOM Server project with an IP address and port number, where the HELCOM Server can connect to the AIS service.

Data subscribers can test the connection to the HELCOM server, but cannot expect a continuous data stream to be available, since full security measures will not be in place and bandwidth is not yet available for full operational load.

To provide a minimum of security in this period, the HELCOM server will always connect from the HELCOM_IP address, so each participating party can protect their network with a firewall, and only allow connects to this port from this specific IP address. Similarly, participating parties will only be allowed to connect from one specific IP address.

Please make sure, that if there is a firewall between the suppliers AIS system and the internet, the firewall is configured to allow connects from the HELCOM_IP address through to the relevant port number on the suppliers AIS service.

Scenario 2: Beta-release period (February – May 2005)

When the HELCOM Server starts the Beta-release period, the participating parties will receive a Client Proxy application (with installation and user manual), which must be executed on a local server. The Proxy Client will connect to the HELCOM Server using SSL (Secure Socket Layer), and ensure authentication and encryption of the communication across the Internet.
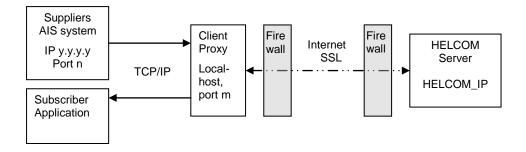

Figure 2: HELCOM server retrieving data via a Client Proxy, using a TCP/IP socket connection between the AIS service and the Proxy.

The participating parties will now connect to the locally executing Client Proxy instead of connecting to the HELCOM Server directly, but still locally using a TCP/IP socket connection.

The main purpose of the AIS Client Proxy is to establish and control a link between the participating parties AIS system and the HELCOM Server. Given an internet line, the AIS Client Proxy establishes the necessary SSL connection to the HELCOM Server.

The core functionality of the AIS Client Proxy program can be divided into the following four sections:

User Authentication Interface

As the system only allows authenticated users to access the HELCOM Server data, the proxy presents a user interface where it is possible to enter the username and password used for the authentication. The entered information is sent to the server which does the actual authentication and decides if the user is allowed to receive AIS data.

Proxy Data

The proxy program will open TCP/IP port 4001 on the client computer (local host ~ IP 127.0.0.1) and start listening for connections from a Subscriber Application. The socket connection between a Subscriber Application and the AIS Client Proxy is opened by the Subscriber Application. When a Subscriber Application connects, dataflow is as follows: HELCOM server –> proxy –> Subscriber Application.

If port 4001 is already used, it can be changed in a local configuration file.

The local IP address and port number of the suppliers AIS system must be configured in the Client Proxy application and from this point on, the Client Proxy will attempt to connect to the suppliers AIS system. As soon as a connection is established and data are received, the dataflow will be as follows: Local AIS system -> Client Proxy -> HELCOM Server.

Security

Because the username and password are transmitted over the internet, it is important that they are protected (encrypted) so it is not possible for hackers to intercept them.

The encryption is handled with SSL.

It is worth noting that the proxy will try to connect to the HELCOM server on port 4000. This port will of course be open on the firewall guarding the HELCOM server. If there is another firewall between the local computer running the proxy and the HELCOM server, the local firewall has to allow connects from the proxy to HELCOM_IP, port 4000, in order to use the SSL solution.

The SSL encryption is enabled by default during the logon procedure where the username and password are sent across the connection.

Simple Status Monitoring

The proxy also enables the user to see a simple view of the system status.

When a problem is detected somewhere in the system, an operator at the HELCOM server can notify all the connected proxies, so the users can see that there is a problem, and that the flow of data might be disturbed.
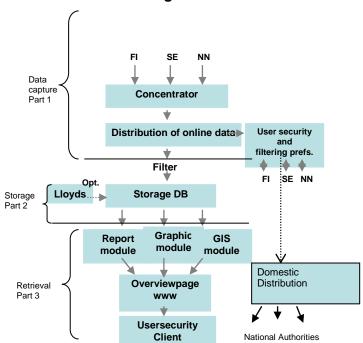
Please make sure that if there is a firewall between the suppliers AIS system and the internet, the firewall is configured to allow connects from the Client Proxy to the HELCOM_IP address.

Internet Connection Bandwidth Requirement

The bandwidth of the internet connection between the AIS data supplier and the HELCOM server needs to be sufficiently large to handle all data without any delays.

Empirical tests show that a bandwidth between 64Kbit/sec and 256Kbit/sec will be sufficient depending on the number of ships. If data are down sampled (i.e. position reports are only delivered every sixth minute or similar) bandwidth requirements will be less.

HELCOM Server Flow diagram

FORM FOR A STANDARD AGREEMENT ON ACCESS TO AND USE OF HELCOM AIS DATA

Preamble

This agreement by and between HELCOM and the Recipient establishes the terms of access to specified HELCOM AIS data.

§ 1   Parties

The Parties to this agreement are:

The Baltic Marine Environment Protection Commission
Helsinki Commission
Katajanokanlaituri 6B
FI-00160 Helsinki

Hereinafter referred to as HELCOM

and

[Insert name and contact details of Applicant]

hereinafter referred to as the Recipient.

§ 2   Background

The HELCOM AIS system consists of a network of national AIS base stations situated in the Baltic Sea Countries and Norway. The information from this network is stored at a designated HELCOM AIS Information Centre, which is maintained by the Danish Maritime Authority.

§ 3   Warranties by the Recipient

The Recipient assures that its use of the HELCOM AIS data is restricted to [insert a purpose of use as applied for] as stated in the application and cf. § 4.

The Recipient further assures that the granted HELCOM AIS data and any derivatives thereof will not at any time be redistributed to or used by any third party except [insert end users of the results and/or derivatives thereof].

The Recipient agrees to share the results of its use of HELCOM AIS data with the relevant HELCOM fora upon request.

Moreover, the Recipient assures that it by all necessary means will protect the granted HELCOM AIS data from any unauthorized use by the Recipient or a third party.

§ 4   Granted HELCOM AIS data

The access to the following HELCOM AIS data is granted:
1) Period covered: [insert date from and to]
2) Data: [mark as appropriate]
      a) Historical data
      b) Statistical data
      c) On-line access to real-time data:
            • Web access
            • Streamed data access
                - Geographical scope:
                - Update rate:
3) Other restrictions to be applied:

§ 5   Duties of HELCOM

HELCOM ensures that the appropriate HELCOM AIS data is available from the HELCOM AIS Information Centre accessible via a secured connection on the Internet and provides information on the log-on procedure including username and password.

§ 6   Disclaimer on behalf of HELCOM

HELCOM makes no explicit or implied warranty as to any matter whatsoever, including the availability, accuracy, or reliability of any information or data, whether tangible or intangible, made, developed or supplied under this agreement, or the ownership, merchantability, or fitness for a particular purpose of the information, of the data made, developed or supplied.

HELCOM does not accept any liability in the event of unavailability of HELCOM AIS data from the system.

§ 7   Entry into force and right of termination of the agreement

This agreement enters into force at the final day of signing, cf. § 9.

The agreement is valid for an unlimited period of time, however, the access to HELCOM AIS data is restricted according to the abovementioned limit in time, cf. § 4.

Both Parties are entitled the right of terminating this agreement upon a formal written notice on the intention of terminating this agreement in total or in part. Such notification on termination must be received by the other party in order to take effect.

The term of notice is six (6) months.

Any failure to fulfil any of the conditions in this agreement entitles HELCOM the right to terminate the Recipient's access to HELCOM AIS data without further notice.

The restrictions for the use and distribution of the HELCOM AIS data are valid after termination of the agreement.

§ 8   Dispute resolution

Any dispute, controversy or claim arising out of or relating to this agreement, or the breach, termination or validity thereof shall be finally settled by arbitration in accordance with the Arbitration Rules of the Finnish Central Chamber of Commerce.

The choice of law will be made in accordance with the Rome Convention 1980.

The Rules of the Arbitration Institute of the Central Chamber of Commerce of Finland is deemed applicable.

§ 9   Signature

This agreement has been drawn up in two (2) identical originals; one for each party.

On behalf of HELCOM

[Insert place and date]
[Insert name and title]

On behalf of the Recipient

[Insert place and date]
[Insert name and title]