European Maritime Safety Agency

Med AIS Workshop no 4
Lisbon 6 June 2007

STIRES 4/MED/8
3 & 4 July 2007

Access Rights

Submitted by EMSA

Executive summary	For the information of the participants, the paper offers the following information: Annex I, SSN/6/4/1 the latest version of the agreed access rights for SSN; and Annex II, the Helcom Agreement on Access to AIS-Information.
Action to be taken	As per paragraph 2
Related documents	SSN.6/4/1 available from the EMSA website with the report on implementation given in SSN.7/4/6.

1. INTRODUCTION

This paper is offered as background for the information of the participants, in:

Annex I, SSN/6/4/1 the latest version of the agreed access rights for SSN (implemented in SSN Version 1.9); and

Annex II, the Helcom Agreement on Access to AIS-Information for the Baltic Region.

2. ACTION REQUESTED

The participants are requested to note the contents of the attached annexes as a contribution towards improvement in the development of the Mediterranean AIS Regional Server.

European Maritime Safety Agency (EMSA)
Av. Dom João II, Lote 1.06.2.5, 1998-001 Lisbon, Portugal
Tel: +351 21 1209 278, Fax: +351 21 1209 217

Annex I

SafeSeaNet Access Rights (SSN/6/4/1)

1. INTRODUCTION

At ISWG 3, EMSA submitted document 3/4/1 that recommended several modifications regarding the management of the Users' Access Rights. The document aimed to address a concern raised by Member States questioning SSN's compliance with the initial system requirements.

The outcome of the discussion is summarised in the ISWG 3 Conclusions document. Two main requirements emerge:

- It is the responsibility of the MS to manage the access rights at the NCA level,
- It is the responsibility of SSN to guaranty that the requestor has the relevant access rights.

The present document is based on these two statements together and taking into account the Network and Security Reference Guide v1.14 and the Interface Control Document (ICD), Issue 1, Revision 0

2. EMSA COMMENTS

2.1. General

In order to progress with this rather complicated task a revision of the SSN User Access Rights management needs to be slightly modified to achieve the requested flexibility.

Much of the problems encountered is connected to the use of Locode as a user identifier (as an ID). As long as we don't have a single Locode for the port authority in a port area, it is well known that in many Member States a larger port area can have several Locodes, it will result in a need of several user IDs for one port authority to be able to have a complete traffic overview for the hole area.

A solution could be to have a user ID disconnected from the Locode system, where we could cluster Locodes to one user ID. Then we also would have solved the problem with the main port and sub port operation.

The solution proposed by the ISWG was to create a matrix solution that could be operated at NCA level. This would give the requested flexibility for the member states, but it caused also some discussion how to manage that only legal authorities get access to more sensitive information like Security Notifications.

To operate this type of flexibility EMSA needs to develop a more elaborated User Manual that clearly states how to create the different types of roles under the NCA responsibility and the legal condition behind each role.

European Maritime Safety Agency (EMSA)
Av. Dom João II, Lote 1.06.2.5, 1998-001 Lisbon, Portugal
Tel: +351 21 1209 278, Fax: +351 21 1209 217

2.2. SSN Roles

The present Network and Security Reference Guide (NSRG) (see page 37) states that every SSN user is assigned a single role in SSN. Each of these roles is assigned a set of default and maximum access rights.

> A further statement is: "Roles access rights are managed at the project level by the system administrator and can only be modified by a change request submitted by the DG-TREN". EMSA is operating SafeSeaNet on behalf of DG-TREN.
>
> Based on the existing documents a new Role can not be created by a Member State directly. Approvals for a new Role have to be made by EMSA. An intervention on system (in the present system) level will also be necessary for certain rights connected to a "mixed" role.
>
> At present this is a legal and practical boundary for the SafeSeaNet system.

2.3. Concerns expressed during previous workshops.

According to the NSRG page 38, a port authority may only obtain information from SSN if the next port of call within the requested information can be identified as their port.
Several Member States confirmed that this rule does not function within the SSN system.

Member States requested clear assurance that the system would not allow any LCA to receive port notifications for places for which that LCA is not the port authority or is not allowed to act on behalf of the port authority. This rule does not currently function in the SSN system.

Member States requested in certain cases national arrangements, larger ports be permitted to send notifications on behalf of smaller ports. An evaluation of the correction to SSN that would be required has been provided by EMSA's contractor. An implementation of this requirement would necessitate substantial important modifications to the current SSN system and present a high risk in case of the current version, SSN V1.83.

These concerns are connected to the present system. When SSN starts to deal with Security Notifications a clear specification of roles will be even more important.

3. ISWG3 PROPOSAL

The participants in ISWG3 agreed that a more flexible arrangement for access rights were necessary to fulfil their obligations in a proper and efficient way. Further, it is necessary to make SSN more user friendly in daily use.

Based on the arguments presented during the discussion, EMSA has developed the following proposal.

- Based on the legal requirements in Network and Security Reference Guide v1.14
- Based on the legal requirement in Interface Control Document (ICD), Issue 1, Revision 0

European Maritime Safety Agency (EMSA)
Av. Dom João II, Lote 1.06.2.5, 1998-001 Lisbon, Portugal
Tel: +351 21 1209 278, Fax: +351 21 1209 217

- EMSA develop a Role Matrix, which can be used by the Member States to specify their needs for a specific role that comply with operational requirement connected to a specific LCA.
- The Role Matrix have to be sent to EMSA for approval and technical validation (what is possible in the present system)
- If any changes are needed the Member State is contacted for consultations.
- After agreement, EMSA create the new Role and inform the NCA involved.

Experience gained from this process, EMSA will take this into consideration when introducing system modifications or when new system versions are developed. We have to recognise that the present system has rather limited possibility to permit a flexible and user friendly solution.

4. THE ROLE MATRIXES

In the Access setup environment for SafeSeaNet we have three elements.

1. The first element is the ID and the password that specify the person that shall have access. Based on the authentication and authorisation rules we know that this person is connected to an authority and the legal condition is approved by NCA or EMSA.
2. Element two is the functionality. To perform different activity in SafeSeaNet we need to have access to different functionality. Even if this in fact consists of two elements we treat it as one. These two are function and type of information connected to the function. To illustrate this we can take a look at sending notification. The function it self is to send a notification. In addition to this functionality we also define which type of information that the person can transmit. We have exactly the same situation for the request functionality.
3. Element three is area, for which the person has right to notify or request information. Until now this element has been integrated into element two (the present role definition). This lack of flexibility has created some frustration for Member State users. The objective for the proposal in this document is to create a more flexible solution that is easier to adapt to the practical life.

   What we have done is only to break the link between the functionality and the area and specify them individually.

To specify the complete access rights for a Member State user, two matrixes are developed, one for functionality and information type and on for area access. This gives the NCA the needed flexibility to combine area and functionality for each user so it fit with the operational situation for that specific authority.

The matrixes are presented on the next pages. A xls file is made for requesting functional and area access rights.

5. EMSAS PROPOSAL FOR NEW ROLE MATRIX

Based on the above mentioned, the following matrix is developed to fulfil the requirement for requesting a new role.

European Maritime Safety Agency (EMSA)
Av. Dom João II, Lote 1.06.2.5, 1998-001 Lisbon, Portugal
Tel: +351 21 1209 278, Fax: +351 21 1209 217

The present Role Matrix

	Send Notification (WEB/XML)									Information Requests (WEB/XML)										Information Requests (WEB Only)					
										Notification Details										Ship Search				Port Search	Area Search
	Port	Ship	Hazmat	Security	Alert					Port	Ship		HAZMAT	Security	Alert					Latest Notif	Voyage	Cargo Manifest	Latest Incidents		
Roles					SITEREP	POLREP	Waste	L/F Containers	Others		MRS	AIS			SITEREP	POLREP	Waste	L/F Containers	Others						
POR	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[1]	Y[1]	Y[1]	Y[1]	Y[3]	N	N	Y	N	N	Y[1]	Y[1]	Y[1]	Y	Y[1]	N
CST	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[3]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y/N	Y
PSC	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
NCA	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
EMSA	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
MIN	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	Y
All	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
OTH	N[2]	N[2]	N[2]	N[2]	N[2]	N[2]	N[2]	N[2]	N[2]	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y

[1] If the Port Authority is the next port of call

[2] The granting of an access right would have to be decided on a case by case basis, depending notably on the relevance of the information for the authority or body concerned, and taking into account protection of confidentiality.

[3] To be confirmed (such authorities may have not yet been defined)

Others: Could be represented by Customs, Schengen and others.

European Maritime Safety Agency (EMSA)
Av. Dom João II, Lote 1.06.2.5, 1998-001 Lisbon, Portugal
Tel: +351 21 1209 278, Fax: +351 21 1209 217

Request Role Matrix

NCA Role Request Form

	Send Notification (WEB/XML)									Information Requests (WEB/XML)									Information Requests (WEB Only)						Administration				
										Notification Details									Ship Search				Port Search	Area Search	Manage				Request
Roles	Port	Ship	Hazmat	Security	Alert					Port	Ship		HAZMAT	Security	Alert				Latest Notif.	Voyage	Cargo Manifest	Latest Incidents			LOCODE Register	Vessel Register	Manage Roles	Manage Users	Statistics
					SITEREP	POLREP	Waste	L/F Containers	Others		MRS	AIS			SITEREP	POLREP	Waste	L/F Containers	Others										
NCA Access Rights ==>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	Y
Requested Access for:																													
Role 1 ==>																													
Role 2 ==>																													
Role 3 ==>																													
Role 4 ==>																													
Role 5 ==>																													
Role 6 ==>																													

<=> Can be decided by NCA — Type Y or N in all fields of this colour.

<=> Restricted to specific operational status — Type Y or N in all fields of this colour.

<=> Access right Not permitted

European Maritime Safety Agency (EMSA)
Av. Dom João II, Lote 1.06.2.5, 1998-001 Lisbon, Portugal
Tel: +351 21 1209 278, Fax: +351 21 1209 217

Role – Locode table

Cluster of Locodes connected to the Role

Add the Locodes involved

Tick off which Locodes is involved in each Role.

Check whether the Locode is present in SSN and tick off.

LOCODES		Registered in		Role 1	Role 2	Role 3	Role 4	Role 5	Role 6
Country Code	LOCODE	EMSA Level	National Level	Pattern of	Pattern of	Pattern of	Pattern of	Pattern of	Pattern of

Name of Role 1=
Name of Role 2=
Name of Role 3=
Name of Role 4=
Name of Role 5=
Name of Role 6=

Update

6. ACTION REQUIRED

Member States are invited to note the above proposals and to advise as to the appropriate action to take.

Annex II

Helsinki Commission

Agreement in Access to AIS-Information

HELSINKI COMMISSION
Baltic Marine Environment
Protection Commission

AGREEMENT ON ACCESS TO AIS-INFORMATION

Following the HELCOM Copenhagen Declaration adopted on 10 September 2001 to enhance the use of AIS and the implementation of HELCOM Recommendation 22E/5 by the parties the following Agreement has been made between

The Royal Danish Administration of Navigation and Hydrography, representing the Danish party, established in Copenhagen, Denmark

AND

The Estonian Maritime Administration, representing the Estonian party, established in Tallinn, Estonia

AND

The Finnish Maritime Administration, representing the Finnish party, established in Helsinki, Finland

AND

The Federal Ministry of Transport, Building and Housing, representing the German party, established in Bonn, Germany

AND

The Latvian Naval Forces, representing the Latvian party, established in Riga, Latvia

AND

The Lithuanian Maritime Safety Administration, representing the Lithuanian party, established in Klaipeda, Lithuania

AND

The Norwegian Coast Directorate[1], representing the Norwegian party, established in Aalesund, Norway

AND

The Polish Maritime Administration, representing the Polish party, established in Warsaw, Poland

[1] Norway, not a Contracting Party to HELCOM, via its administration, the Norwegian Coast Directorate enters into this agreement accepting the full and mutual responsibilities following to this agreement.

AND

The Russian Federal Agency of Maritime and River Transport, representing the Russian party, established in Moscow, Russia

AND

The Swedish Maritime Administration, representing the Swedish party, established in Norrköping, Sweden

Preamble

At the HELCOM Extraordinary Ministerial Meeting in Copenhagen on 10 September 2001 it was 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". The Terms of Reference for the Working Group also comprise the task to "consider the legal framework and find solutions for the handling and use of AIS-data exchanged between the Baltic States".

The participating parties have now agreed on the methods for exchange of AIS-data and the implementation of the system has started.

Definitions

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

Objective

This Agreement regulates the 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 regulates the distribution and use of the AIS-data received from the Participating parties.

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 AIS data

Each Participating party must restrict the distribution of received AIS-data to their own organisations and other competent authorities. AIS-data may only be used for purposes listed in **Appendix 1** without written consent from the party that has delivered the AIS-data.

Each Participating party is responsible for the use of AIS-data by their competent authorities. The Participating parties must take appropriate actions to ensure that the competent authorities do not redistribute AIS-data to a third party and that AIS-data only is 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.

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 and also to other applicable international, European Cmmunity and national law and regulations.

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 Agreement, 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 this Agreement, 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 fulfil any of the conditions in this Agreement gives the sending or transmitting party right to terminate access to AIS-data for as long as the receiving party is in breach of the condition.

Changes to the Agreement

Changes to this Agreement shall be agreed in writing between the parties.

Disputes

In case of a dispute between Participating parties as to the interpretation or application of this Agreement, they should seek a solution by negotiation. If the parties concerned cannot reach agreement, they should seek the good offices of or jointly request mediation by a third Participating party, a qualified international organization or a qualified person.

If the parties concerned have not been able to resolve their dispute through negotiation or have been unable to agree on measures as described above, such disputes shall be, upon common agreement, submitted to an *ad hoc* arbitration tribunal, to a permanent arbitration tribunal, or to the International Court of Justice.

Termination of the Agreement

This Agreement will be in effect from the date of signature by all of the Participating parties and shall last for a period of five (5) years. Thereafter, this Agreement shall automatically renew for a term of one (1) year.

However, any Participating party may terminate its own participation in the co-operation stipulated in this Agreement giving each of the other Participating parties six months written notice.

This Agreement is done in 10 equal counterparts, retained by each of the Participating parties.

Appendix 1

APPLICATIONS FOR RETRIEVED AIS DATA FROM THE COMMON BALTIC SEA AIS MONITORING SYSTEM

Only competent authorities shall have access to the common Baltic Sea monitoring system and these authorities shall only be allowed to use retrieved AIS data for the applications specified below.

Operational requirement on AIS Shore stations regarding information to other countries

Interest for the littoral state to get information; only locally (L), from adjacent countries (A), from total Baltic area (C)
Needed update rate from SOLAS ships; full update rate (1), once every 6 min (2), once every week or more (3), not permanent, at request (4), Statistic data to be shown or to be down loaded at request (5)
If access to a full update rate is needed this should be solved on a bilateral basis.

Information			Rate	Functionality	Accessibility	
						HELCOM
		C	2,5	No direct access req.	HELCOM secretariat	1. Statistics 1.1. Call sign 1.2. Position 1.3. Cargo 1.4. Etc...to be determined
						National competent authorities
L	A	C	1,2,3	Bi-directional communication*	Countries involved	1. Pollution combating
L	A	C	1,2,3	Bi-directional communication*	Countries involved	2. *Contingency planning*
L	A	C	1,2,3	Bi-directional communication*	Countries involved	3. *International Ship and Port security (ISPS)*
						SAR
L	A	C	1,2,3	Bi-directional communication*	Countries involved, MRCC	▪ To supply the on-line information for SAR needs, including adjacent sea areas, to get an overall traffic picture ▪ To search for a specific ship in the HELCOM data base

						VTS
L	A	C	1,2	Bi-directional communication*	Adjacent authorities, VTS centres	Traffic management etc.
						Paris MOU (Port state control)
		C	2,4	Only listening	Port State Control authorities	Monitor and compare against banned ships.
						EU HAZMAT reporting requirement
L	A		2,4			1. Mandatory reporting system
						Ice Breaker Service
L	A	C	1,2	Bi-directional communication*	Competent authority and Ice Breakers	To get a holistic assessment of the conditions and of the speeds of ships in ice covered waters
						Port Authorities
L	A	C	1, 2	Only listening		Filtered information for ships entering or leaving the port

The table requires further consideration to define in detail information to be exchanged among parties concerned.
* To be determined. Not to be applied for the demonstrator.

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 e.t.c. 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 project manager Jens Kristian Jensen jkj@frv.dk 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.

Table of Contents

INTRODUCTION 1

PURPOSE 1
SCOPE 1
Scenario 1: Testing and preparation period (October 2004 – January 2005) 1
Scenario 2: Beta-release period (February 2005 – May 2005) 1
TABLE OF CONTENTS 2
REFERENCES 2
DEFINITIONS, ACRONYMS, AND ABBREVIATIONS 3

INTERFACE DESCRIPTION 3

DATA FORMAT 3
SECURITY 3

CONNECTION SETUP 4

SCENARIO 1: TESTING AND PREPARATION PERIOD (OCTOBER 2004 – JANUARY 2005) 4
SCENARIO 2: BETA-RELEASE PERIOD (FEBRUARY – MAY 2005) 5
User Authentication Interface 5
Proxy Data 5
Security 6
Simple Status Monitoring 6
INTERNET CONNECTION BANDWIDTH REQUIREMENT 6
HELCOM Server Flow diagram 7

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)

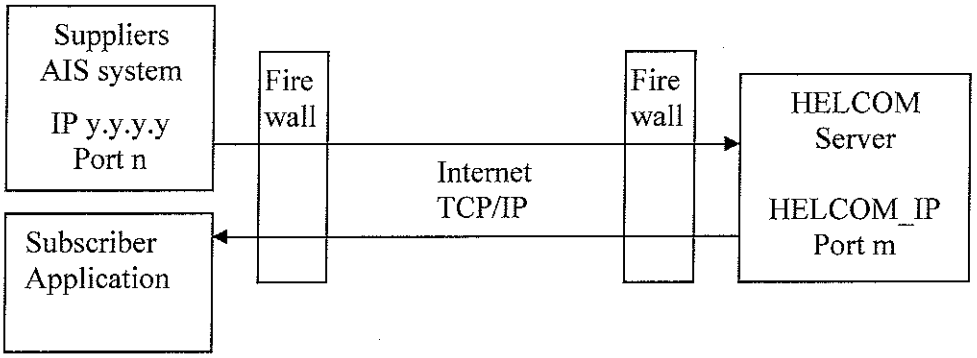

Figure 1: HELCOM server retrieving data over a TCP/IP socket connection.

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.

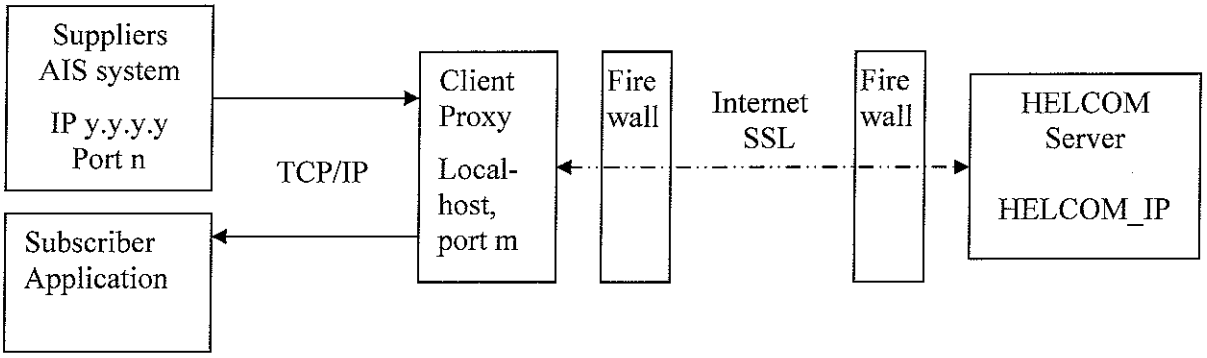

Figure 2: HELCOM server retrieving data via a Client Proxy, using a TCP/IP socket connection between the AIS service and the Proxy.

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