Med AIS Workshop no 4
Lisbon 5 June 2007

STIRES 4/MED/6
3 & 4 July 2007

Med AIS Specifications

Submitted by Italy

Executive summary	Provides details related to the specifications for the AIS Mediterranean Regional Server in four parts (as attachments): (1) Operational & technical requirements; (2) Helcom/Med Comparison table; (3) System demonstrator; and (4) Security.
Action to be taken	As per paragraph 3
Related documents	Actions from the report of the 3rd Med EWG, STIRES 4/MED/2.

1. INTRODUCTION

This paper (with four attachments) supports the presentation for information the specifications for the Mediterranean AIS server to the Member States participating in the Regional system. This is supported by actions identified at previous EWG meetings and the EMSA – Italy meeting of 2nd May 2007. STIRES 4/MED/6 (3) System demonstrator contains a new proposal, but in line with development of the Baltic/Helcom system. It also includes specific action for the third meeting:

"d. On the levels of security of the data, Italy would be responsible for gathering more information on this issue area and more would be presented at the Med AIS EWG 4."

2. ATTACHMENTS

These are:

STIRES 4/MED/6/1 Operational & technical requirements;

STIRES 4/MED/6/2 Helcom/Med Comparison table;

STIRES 4/MED/6/3 System demonstrator; and

STIRES 4/MED/6/4 Security.

3. ACTION REQUIRED

The Member States are invited to note, consider and support the proposals contained in the four attached documents.

GUARDIA COSTIERA

4th Mediterranean EWG

Document n. 4/1 Vers. 1.1
Lisbon, 3-4 July 2007 June 5th 2007

AIS MEDITERRANEAN REGIONAL SERVER

Operational and technical requirements

1. Scope

This document describes the technical requirements of a Mediterranean regional server for exchanging data between the AIS national server of the following littoral States:

- Bulgaria;
- Croatia;
- Cyprus;
- France;
- Greece
- Italy;
- Malta;
- Portugal;
- Romania;
- Slovenia;
- Spain;
- Turkey.

2. References

This document has been written taking in consideration the following references:

- ITU Recommendation on the technical characteristics for a universal shipborne Automatic Identification System (AIS) using time division multiple access in the Maritime Mobile Band (ITU-R M. 1371-2);
- IALA Technical Clarification on ITU-R M. 1371-1 (ed. 1.5, 2006);
- IEC Standard 61162-1: Maritime navigation and radiocommunication equipment and systems – Digital interfaces;
- IEC/PAS 61162-100: Maritime navigation and radiocommunication equipment and systems – Digital interfaces Part 100: Single talker and multiple listeners – Extra requirements to IEC 61162-1 for the UAIS;
- IEC/PAS 61162-101: Maritime navigation and radiocommunication equipment and systems – Digital interfaces Part 101: Single talker and multiple listeners – Modified sentences and requirements for IEC 61162-1;

- IEC Standard 61993-2: Class A Shipborne equipment of the Universal Automatic Identification System (AIS) - operational and performance requirements, methods of testing and required test results;
- IEC Standard 62320-1: AIS Base Stations - Minimum operational and performance requirements, methods of testing and required test results;
- IALA Recommendation A - 124 on AIS Shore Stations and Networking Aspects Related to the AIS Service;

3. Introduction

The main functions of a regional AIS server are:

-collecting,

-distributing,

-displaying,

-storing

AIS data coming from the national systems which are connected to the regional server.

The most important service that a regional AIS server provides is the reception of AIS data in real time and the storage of the incoming data; so the implementation of a regional AIS server requires permanent connections with all the national AIS servers to allow the exchange of data between the systems involved.

The whole image of the collected data, or part of it, is sent back in real time to each state, depending on its requirements. The stored data are used to produce statistical reports which can be viewed using tables and diagrams or layered over charts (GIS).

4. Architecture

The architecture of the regional system must be divided in two separate segments. The first segment includes software modules that must be installed on hardware located inside the national borders of each participant State (PS).

The location where this hardware will be placed can be decided by the National Authority involved; this part of the system will be the gateway (*Proxy*) which enables the AIS data exchange between each national system and the regional server.

The second segment includes software modules that must be installed on server(s) which will be located in the regional center placed in the Italian Coast Guard Headquarters. The main services which must be provided by these modules are:

-collecting and distributing AIS data from/to the PS;

-storing AIS data in the regional database;

-retrieving and analysing the stored AIS data and displaying these data in predefined reports, in diagrams and layered over charts (GIS).

Internet will be used for connecting the regional server with the national proxies.

The regional system must be designed to sustain the data produced by the vessels inside the Mediterranean Sea area. As of today, we can estimate that there are 20,000 vessels on which the AIS is or will soon be installed.

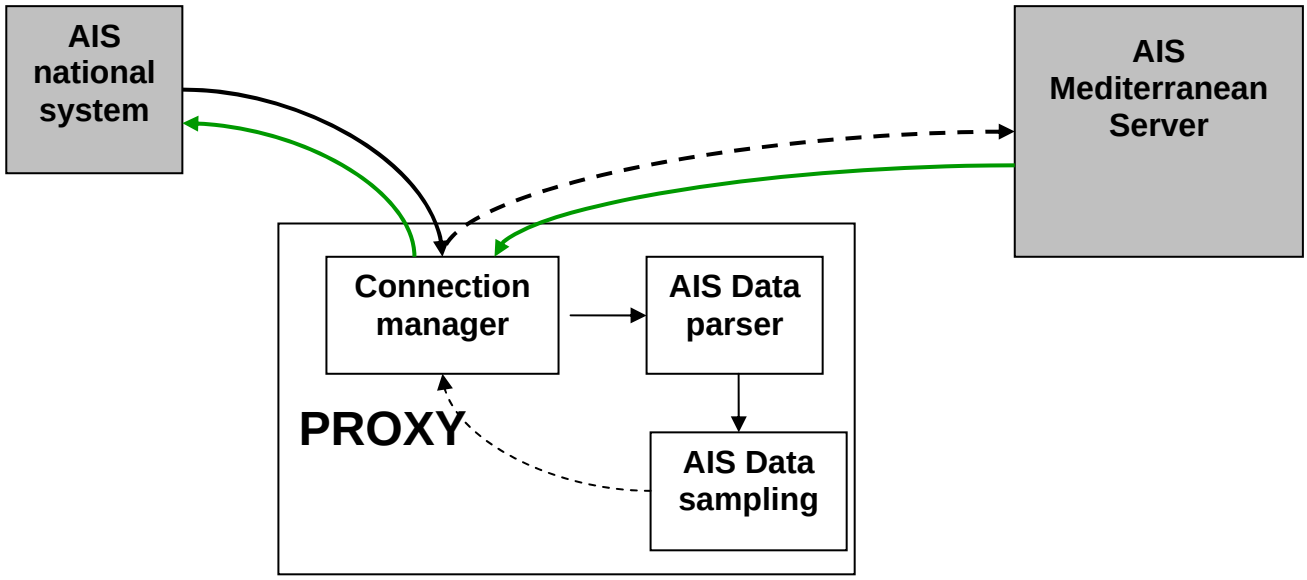
The dynamic data which the class A AIS transmits are forwarded using a standard IEC 61162 sentence which is 50 bytes long. Static and voyage data of a class A AIS are forwarded using a standard IEC 61162 sentence which is 115 bytes long. In addition, we must account for an additional field to add the timestamp of reception to each sentence; this field can be implemented with a 4-bytes integer representing the number of seconds elapsed from a common reference time. In conclusion, the whole set of data of a class A AIS can be forwarded using:

$$D = 50+4+115+4 = 173 \text{ bytes} = 1384 \text{ bits}$$

Therefore, we can estimate the minimum requirements for the Internet connection bandwidth to allow the exchange of all the regional AIS data:

$$\text{RegBW} = \frac{20000 \cdot 1384}{360 \cdot (1 - X)} \approx 200 \text{ kbits/s}$$

where X, which represents the bandwidth margin which accounts for the transmission over the Internet and the utilization of security protocols, has been assigned the value of 0.6, and where a transmission of the complete AIS data for each target occurs every 360 seconds.



These estimations must be used in the act of defining the minimum requirements for the hardware, the architecture of the software modules and the network infrastructure.

5. Functional Characteristics of National Proxy

The main function of the national proxy is to establish and manage the connection between the national system and the regional server. In particular, the proxy should guarantee a secure connection to the regional center. The national application which is connected to the proxy must establish the connection through *username* and *password* authentication. Data exchanged between the proxy and the regional server must be encrypted through the use of SSL/TSL connections.

The format of the exchanged AIS data must comply with the IEC 61162-1, IEC/PAS 61162-100 and IEC/PAS 61162-101 standards. These standards define how AIS data received from AIS targets, through the messages described in ITU-R M.1371, must be encapsulated in a VDM sentence. The IEC 61993-2 standard provides a detailed description of the encapsulation process.

The following sections describe the main functions which the Proxy must implement.

5.1 AIS Data Parser

The proxy must filter the AIS data coming from the national system. In

particular the following data should be filtered:

-sentences other than VDM;

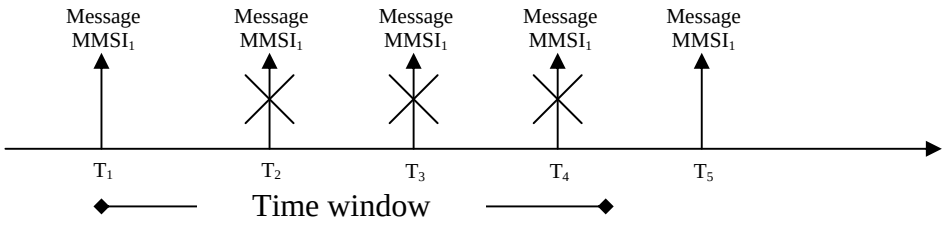
-wrong VDM sentences (not complying to IEC standards);

-VDM sentences which encapsulate ITU messages not required.

The required ITU messages include the messages carrying static, dynamic and voyage AIS data (i.e. ITU messages 1, 2, 3, 4, 5). Means must be provided to configure filtering rules to extend data forwarding to other ITU messages when required; for example, the ITU messages 9, 18, 19, 24A and 24B should be added to extend the AIS data exchange to SAR and class B AIS in the next future.

5.2 Sampling

The proxy performs a sampling of the national AIS data before sending them to the regional server. In particular, for each AIS target (targets are identified by MMSI) a single set of data must be forwarded to the regional server inside a predefined time window. The following picture graphically represents the decimation function.



The time window should be 360 seconds wide by default. Moreover, it must be possible to change this value for each required ITU message. In fact, it can be required to perform a weaker decimation on some kind of messages (for example, message 9 which is transmitted by SAR aircrafts.

5.3 Connection to the Regional Server

Internet will be used for connecting the regional server with the national proxies.

The *Proxy* must establish and manage the connection to the regional server. Once the connection is established, it must handle the transmission of decimated data originating from the national system to the regional server. Likewise, the *Proxy* must route the composite data originating from the regional server towards the national system.

The data exchange between the *Proxy* and the regional server must use secure connections based upon SSL/TSL protocols. Moreover, to improve the security of the data exchange on the Internet, only static IP addresses will be used, so the participant States can protect their networks with a firewall.

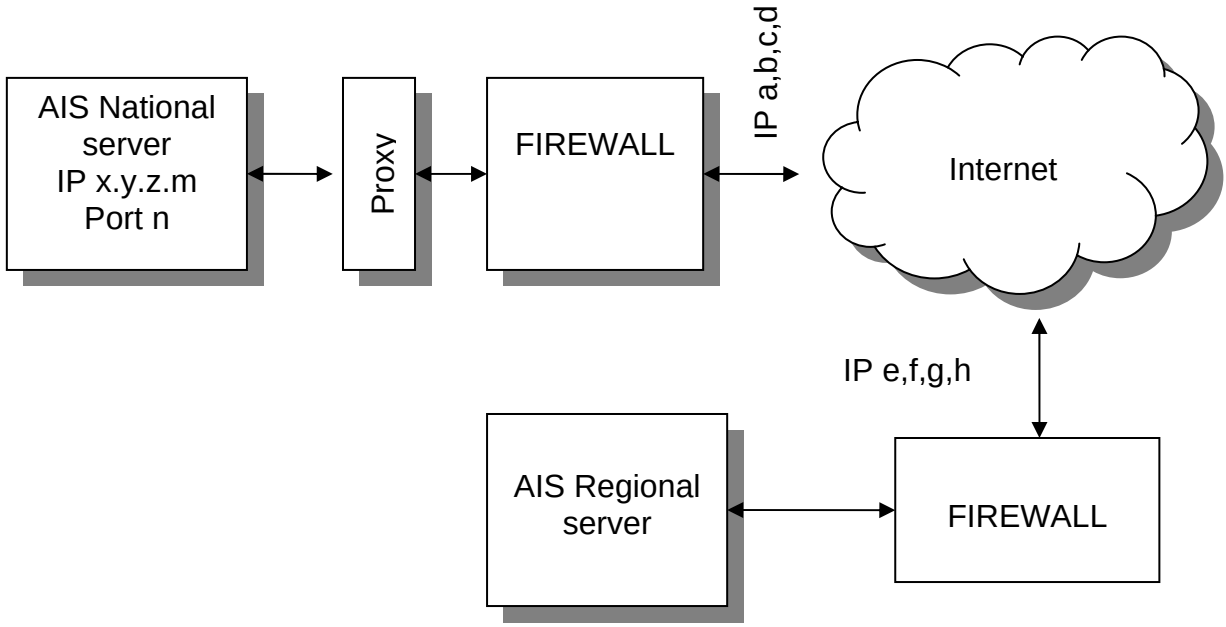


Fig. 2

6. Regional Server Functional Characteristics

The regional server must be always connected through the *Proxies* to all the national AIS systems. The main functions of the regional server are collecting, distributing and storing the AIS data. Moreover, external users must be allowed to display the stored AIS data through a web client.

In conclusion, the regional server must perform the following main services:

-collection of data from the national *Proxies*

-distribution of data towards the national *Proxies*

-storage of data in the regional database

-displaying and statistical processing of data through web portal.

6.1 Data Collection

This functional module collects the AIS data from the connections towards all the national *Proxies*. Moreover, it must perform filtering of data in order to remove possible duplicates caused by repetitions of the same AIS track; the presence of these duplicates is due to acquisition of the same target by different national AIS systems.

The combined flow of AIS data originating from the aggregation of the national data streams must be routed towards the regional database for storing and towards a functional module which must deal with distributing the combined data to the national systems.

6.2 Data Distribution

This functional module must send the AIS data collected by the regional center to the national systems linked through the connection with the *Proxies*. It must be possible to select a subset of the collected data for each member state on the basis of geographical criteria. In addition to this, it must be possible to set a decimation rate of the outgoing data that is different for each member state.

6.3 Data Storage

The main service offered by the regional database is storing the combined image of the AIS data. Stored data must be made available for playback displaying and for statistical report generation.

The arrangement of stored data must be designed to offer these services, keeping into consideration that the number of AIS-equipped vessels is estimated in about 20,000 units.

6.4 Data Displaying and Processing

Access to AIS data stored in the regional database must be managed through a dedicated web portal. This solution allows users to display AIS data using commonly available browsers, such as Internet Explorer. Control of data

access must be provided through authentication by means of *username* and *password*. The connection must be secured through SSL/TSL (HTTPS). The system administrators must be able to define the access rights for each user with the purpose of limiting access to a subset of the stored data. The list of enabled users and their access rights are managed at a regional level.

The web interface must provide the user with a picture of the ongoing traffic in a given area. Minimum requirements for this visualization are:

-displaying of AIS targets upon maps generated by GIS software

-playback function to display historical data

-filtering function to limit the number of displayed targets to a user-definable subset. Filtering can be performed against each of the fields defined by ITU for AIS targets, like name, call sign, MMSI, speed over ground, and so on.

Moreover, the web interface must provide the user with the tools required to perform statistical reports upon the stored data. A number of simple criteria to select AIS data which are of interest for the report are defined:

-**geographical criterion**: all the AIS targets which have crossed or are inside a defined area

-**time criterion**: all the AIS targets received in a user-defined time window

-**field search criterion**: AIS targets that match user-defined values for the following fields:

<type of vessel>
<dimensions>
<cargo type>
<SOG>
<COG>
<name>
<MMSI>
<destination>
<draught>

A query may contain one or no geographical criterion, one time criterion and any number of user-defined field search criteria; criteria are used in logical AND.

Reports must be shown in different formats based upon user preferences.

Table reports must display the AIS data fields listed above. It must be possible to export the table in a format compatible with the commonly available spreadsheets.

Graphical reports must allow the generation of diagrams like histograms, pie diagrams, and so on, based on data selected by a query, to ease statistical analysis.

Fields available for graphical reporting are:

-country flag (embedded in the MMSI number)

-type of vessel

-cargo type

-dimensions

-destination

Geographical reports must display the results of a query on a chart. The kind of representation may be one of the following:

-drawing of vessel routes (by means of dots)

-displaying of traffic density

7. Documentation

A simple user's manual in English will be distributed.

GUARDIA COSTIERA

4th Mediterranean EWG

Document n. 4/2 Vers. 1.0

Lisbon, 3-4 July 2007 June 5th 2007

HELCOM - MEDITERRANEAN SERVER
Comparison Table

1. Scope

In the annexed document has been reported a comparison table between the HELCOM and the planned Mediterranean Server.

2. Legend

The comparison has been performed by several items assembled in the following sets:

- proxy;
- regional server;
- statistics;
- web interface

The result of the comparisons may be:

- (C) – compliancy;
- (V) – variation;
- (A) – addition.

REGIONAL AIS COMPARISON TABLE

FUNCTIONALITIES	HELCOM	MEDITERRANEAN SERVER	INDICATION
Interface with National AIS networks	Proxy based	Proxy based	(C)
PROXY			
User authentication	Yes	Yes	(C)
Data security	Yes, SSL	Yes, SSL	(C)
Exchange data format	IEC 61162	IEC 61162	(C)
Data message forwarding to regional server	All messages	Configurable filter	(V)
Data sampling	Decimation is configurable but it's the same for all ITU messages	Decimation is configurable for each ITU message	(V) & (A)
Access & configuration	Application with GUI interface	Application with GUI interface	(C)
REGIONAL SERVER			
Configuration of user rights	Yes	Yes	(C)
Filtering on data incoming from national proxies	Duplicate removal	Duplicate removal	(C)
Filtering on data forwarded to National Proxies	Yes, filters are defined on a per user basis.	Yes, filters are defined on a per National Proxy basis.	(C)

Filtering on data accessed by Web user	Yes, filters are defined on a per user basis.	The following filters are provided: - target nationality; - target typology; - area; - originator.	(C)
Sampling on data forwarded to users	Yes, configurable on a per user basis	Yes, configurable on a per user basis	(C)
Database back-up facilities	Yes	Yes	(C)
System monitoring	Yes	Yes	(C)
Data Purging	No	Yes	(A)
STATISTICS			
Statistics	Yes, via a web interface	Yes, via a web interface	(C)
Crossing line/Passage line	Yes, with predefined and limited in number lines	Yes, the line can be drawn by the user	(V) & (A)
Crossing areas	No	Yes, areas can be drawn by the user	(A)
Density statistics on AIS fields	Yes. Cargo type, ship type, SOG, draught, destination only at a predefined passage line	Yes. The following functionalities are envisioned: - cargo type; - ship type; - SOG; - draught;	(V) & (A)

		- destination; - number of targets on passages trough lines drawn by the user.	
Number of targets crossing a user drawn area	No	Yes	(A)
Number of targets crossing a user drawn area grouped by typology of target	No	Yes	(A)
Number of times that a specific target cross a user drawn area	No	Yes	(A)
Definition of a geographic filter for computing statistics	No	Yes	(A)
Traffic density plot	Yes	Yes	(C)
Filters for narrowing data used by statistics	Yes. Cargo type, ship type, SOG, draught, destination, length and width, COG, name and MMSI	Yes. Cargo type, ship type, SOG, draught, destination, length and width, COG, name and MMSI	(C)
Download	Yes. Download of statistics results in PDF file	Yes. Download of statistics results in PDF file and in CSV formats	(V) & (A)
Format of reports	Line plot, bar plot, pie plot	Table, Line plot, bar plot, pie plot	(A)
WEB INTERFACE			
Data security	https	https	(C)
Configuration of user rights	Yes	Yes	(C)

Displaying AIS targets upon GIS maps	Yes	Yes	(C)
Playback function	Yes	Yes	(C)
Works with standard browsers	Yes	Yes	(C)
Manual declutter	Yes	Yes	(C)
Manual & automatic refresh	Yes ?	Yes	(C)
Target attributes visualization	Yes	Yes	(C)
Target history	No	Yes	(A)
Export and print of a target history	No	Yes	(A)
Filter definition and activation	Yes	Yes	(C)
Distance calculation	No	Yes, the system calculates the distance between two points on the map fixed using the mouse or inserting two coordinates	(A)
Layer activation/deactivation	No	Yes, the user can activate/deactivate two different layers: - politics boundaries; - ports.	(A)

Document n. 4/3
Lisbon, 3-4 July 2007

Vers. 1.1
June 5th 2007

AIS MEDITERRANEAN REGIONAL SERVER
System Demonstrator

1. Introduction

1.1 Purpose

The present document briefly describes the “AIS Mediterranean Server” implementation phases. A summary of the system functionalities and the estimated delivery timeframe will be highlighted within the following sections.

1.2 System overview

”AIS Mediterranean Server” is intended to be the main system for gaining, distributing, storing and visualizing AIS data acquired from the various Mediterranean AIS National Systems, as already happens for the Baltic and the North Sea.

The envisioned architecture features a continuous link between the National AIS Systems and the Regional Server.

The above mentioned link will be assured by a system sub-component named “National Proxy”. The National Proxy takes care of the management of all the issues related with the physical connection, the secure data exchange and the decimation of the messages sent from each AIS National System to the Regional Server.

AIS data reaching the “AIS Mediterranean Server” will be transferred to all the Countries joining the program.

Those data will be stored and made available to the system users either as statistics or as the result of a “picture” that is the outcome of tracks represented on an adequate cartography.

The “AIS Mediterranean Server” general architecture is depicted in figure 1.

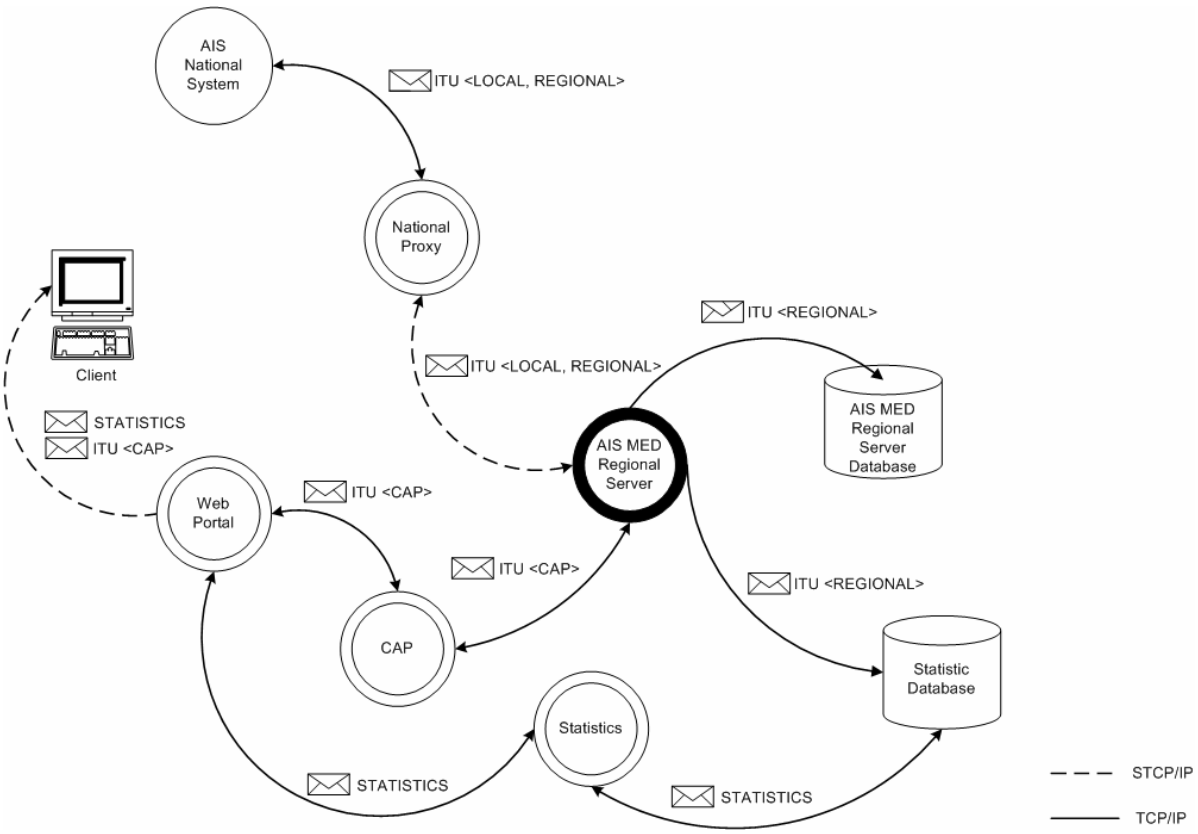


Figure 1 – "AIS Mediterranean Server" general architecture

2. AIS Mediterranean Server implementation phases

The "AIS Mediterranean Server" implementation is envisioned to be performed throughout two consequent phases.

Output of each phase will be an "AIS Mediterranean Server" system release: release 1, also called "Demonstrator" and release 2 (the whole system).

2.1 Phase 1 – System release 1 <Demonstrator>

Aim of system implementation phase 1 is the release 1 of the "AIS Mediterranean Server", also called "Demonstrator".

Purpose of the "Demonstrator" is to provide EMSA with the evidence of the current system implementation. It will also be used to test the system connections, the security solutions adopted and the functionalities developed in a real exercise environment (even if with a limited number of participant Nations).

If the planned activities will be respected (system analysis and design starting on July 2007, feedbacks provided by the buyer as scheduled), we envision to be able to release the "Demonstrator" on April – May 2008.

The regional server release 1 general architecture is depicted in figure 2.

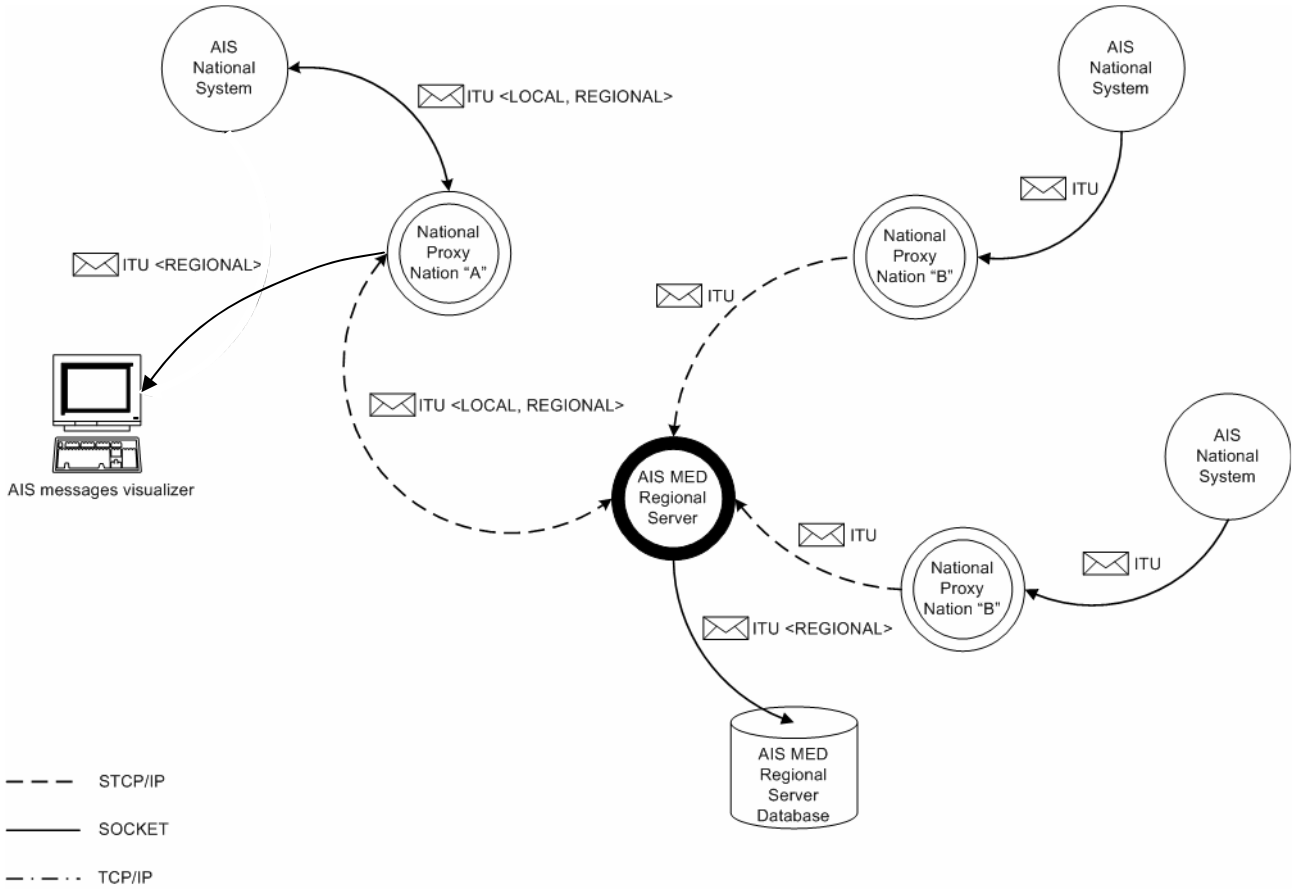


Figure 2 – "AIS Mediterranean Server" release 1 <Demonstrator> general architecture

In order to successfully reach the goals prefixed for the "Demonstrator" we believe the following system sub-components and functionalities should be provided:

(a) National Proxy – "AIS Mediterranean Server" system component that shall take care of the secure connection with the Regional Server and the management and decimation of the AIS messages provided by the "AIS National System". For the purposes of the "Demonstrator" three National Proxies will be delivered

to three different Nations joining the program. For logistics issues we suggest one of the three Nations to be Italy.

(b) AIS Mediterranean Regional Server – "AIS Mediterranean Server" system component that, for the purposes of system release 1, shall take care of the incoming AIS messages collection, redirection and memorization. The "Demonstrator" shall grant the capability to redirect AIS messages gained from the National Proxies connected to one of the three Nations linked. For logistics and organizational issues we suggest to perform the AIS messages redirection to the Italian National Proxy.

(c) Regional Database – "AIS Mediterranean Server" system component that shall be used to store the incoming AIS messages and all the information needed to produce the Combined AIS Picture (CAP).

Moreover, for the purposes of the "Demonstrator" an "AIS Messages Viewer" should be used in order to visualize the AIS Regional Server outputs. The "AIS Messages Viewer" is not part of the present program and is envisioned to be provided by the Italian Coast Guard General Staff.

2.2 Phase 2 – System release 2

Once that the functionalities implemented for release 1 are verified, the implementation of the system will continue: the statistical functions and the web access to the system will be developed. The following additional system sub-components are expected to be delivered:

(a) CAP – "AIS Mediterranean Server" system component that shall take care of the Combined AIS Picture (set of AIS messages collected from all the working National Proxies).

(b) Secure WEB Portal – "AIS Mediterranean Server" system component that shall be used by the system users to access the CAP and request the statistics granted by the system.

(c) Statistics Module – "AIS Mediterranean Server" system component that shall elaborate the statistics functionalities described within the "AIS Mediterranean Server" technical specification document.

(d) Statistics Database – "AIS Mediterranean Server" system component that shall store AIS data in an opportunely organized manner in order to facilitate the data management aimed to statistics purposes.

(e) Client – Component used by the system users to access the Secure WEB Portal. The client is out of the scope of the present document.

If the planned activities will be respected (system analysis and design starting on July 2007, feedbacks provided by the buyer as scheduled), we envision to be able to deliver the whole system in a beta version on September – October 2008. Tests will be performed in order to go live with the "AIS Mediterranean Server" by the end of the 2008.

GUARDIA COSTIERA

4th Mediterranean EWG

Document n. 4/4
Lisbon, 3-4 July 2007

Vers. 1.1
June 5th 2007

AIS MEDITERRANEAN REGIONAL SERVER
Security

1. Introduction

The present document describes the security solutions envisioned for the "AIS Mediterranean Server" implementation. Within the following sections, the security issue is analyzed considering the data security and the proposed connection typology.

The solutions described will be implemented and granted since the release 1 of "AIS Mediterranean Server" <Demonstrator>.

2. AIS data format

The data exchanged among the "AIS National Systems", "National Proxies" and "AIS Regional Server" are formatted in accordance with the following standards: IEC 61162-1, IEC/PAS 61162-100 and IEC/PAS 61162-101.

3. Security

The system to be implemented features the use of two different security levels for the AIS messages exchange:

- AIS messages exchange between "AIS National Systems" and "National Proxies" – AIS messages exchange between "AIS National Systems" and "National Proxies" is based on a TCP/IP connection, by means of an adequate socket.

This solution is adopted envisioning that the AIS data exchange between the above mentioned systems will occur using a secure network infrastructure.

- AIS messages exchange between "National Proxies" and "AIS Regional Server" – AIS messages exchange between "National Proxies" and the "AIS Regional Server" will take place through the employment of protected TCP sockets. Sockets protection is based upon the standard SSL 3.0/TLS 1.0.

The above mentioned protocol, based on the use of digital certificates, grants the transmitted data security by means of specific ciphering algorithms in accordance with the standard.

Within the system architecture proposed, the use of VPN (Virtual Private Network) is not planned. This decision has been taken considering the following factors:

(a) The use of VPN generates complexities in managing the exercise environment. Those complexities are suppose to be inadequate to the system envisioned.

(b) The VPN establishment requires the availability of services and resources that we deem over dimensioned for the system proposed.

(c) The security level assured by the SSL/TLS solution is deemed to be sufficient for the information exchanged typology.

4. Bandwidth

In order to grant a correct AIS messages exchange between the “National Proxies” and the “Regional Server”, without latency on data transmission, a sufficient bandwidth network connection should be allocated at the system disposal.

Considering the average of the AIS messages to be exchanged and the number of AIS contacts concurrently gained (the estimation is about 20,000 contacts per day), the required bandwidth is assumed to be about 256 kbit/sec.

Those assumptions will have to be evaluated and confirmed during the “Demonstrator” testing phase.

5. Connection between “AIS National Systems” and “National Proxies”

The Proxies are software modules installed on hardware located in each Member State that enable the AIS data exchange between AIS National Systems and Regional Server. The exchange of data between the National System and Regional Server is bidirectional.

The data feed from the AIS National System to the Proxy is carried out through a TCP/IP socket connection. In this case, the Proxy can behave either as a server or as a client. When behaving as a server, the Proxy will listen on a configurable TCP port for incoming connections from the AIS National System, while when behaving as a client it

will attempt to connect to the AIS National System at a configurable IP address; in this case the AIS National System will have to act as a server. In either case, once the connection is established the Proxy will forward the data incoming from the AIS National System to the Regional Server.

The data feed from the Proxy to the AIS National System is also carried out through a TCP/IP socket connection. In this case the Proxy behaves as a server, listening for incoming connections from national applications on a configurable TCP port. Once the connection is established the Proxy will forward the data incoming from the Regional Server to the application that requested them.

6. Connection between "National Proxies" and "AIS Regional Server"

The network level connection (TCP/IP Stack) between "National Proxies" and "AIS Regional Server" is established using the IP communication protocol whose protection is granted by the security features of the network perimeter (e.g. firewall, IDS, etc.).

The "National Proxy" and "AIS Regional Server" connection is depicted in figure 2.

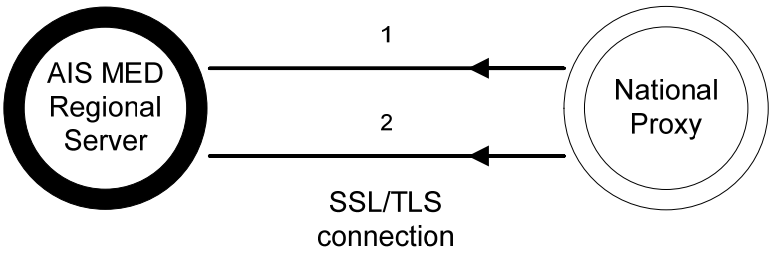


Figure 3 - "AIS Regional Server" and "National Proxy" connection schema

Because the information exchanged will have to transit on an open and un-trusted network (Internet), the solution envisioned features a unidirectional connection client/server style, where the client is the National Proxy and the server is the AIS Regional Server. This connection is based upon the creation of two secure TCP sockets, protected by the use of SSL/TLS (Secure Sockets Layer/Transport Layer Security).

The SSL/TLS solution adopted foresees the assignation to the “AIS Regional Server” of an X.509 v3 digital certificate issued by a Certification Authority accredited at the international level.

Such a digital certificate contains the information related with the “AIS Regional Server” that allows the “National Proxies” to authenticate it in a secure and unique manner before sharing the AIS data.

Sockets to be used for the connection are both established by the “National Proxies” in accordance with the following steps:

(a) The “National Proxy” connects to the “AIS Regional Server” on a specified applicative port.
(b) The “AIS Regional Server” sends its digital certificate to the “National Proxy”.
(c) The “National Proxy” verifies the authenticity and validity of the certificate.
(d) The security parameters are negotiated (key length, protocol, etc.).
(e) The secure socket is created.

Once the secure socket is created the “National Proxy” sends to the “AIS Regional Server” its unique identifier. The “AIS Regional Server” verifies the connected “National Proxy” identity and executes the following actions:

If the verification returns a positive response the “AIS Regional Server” returns an ACK.

If the verification returns a negative response the “AIS Regional Server” closes the connection.

Both of the above described events are registered on specific “log” for the consequent audit.

7. SSL/TLS Performance Considerations

It’s important to consider that performance issues typically involve trade-offs between function and speed. Usually, the more the functions and the processing that are involved, the slower the performance.

The following are two types of Secure Sockets Layer (SSL) functions:

- Handshake.
- Bulk encryption and decryption.

When an SSL connection is established, an SSL handshake occurs. After a connection is made, SSL performs bulk encryption and decryption for each read-write. The performance cost of an SSL handshake is much larger than that of bulk encryption and decryption.

To enhance SSL performance, we have decided to decrease the number of individual SSL connections and handshakes for each National Proxy.

The performance of bulk encryption and decryption is affected by the cipher suite used for an individual SSL connection. To enhance SSL performance, has been adopted the use of the following parameters for the SSL cipher suite:

- RSA ,for Key Exchange.
- MD5, for Integrity Check.
- RC4-128bit, for Data Encryption.