Enhanced Group Call – Application Programming Interface Correspondence Group (EGC-API CG)

Desirable requirements

Version 1.0.0 dated 15 December 2020

Introduction

The International Hydrographic Organization (IHO) World-Wide Navigational Warning Service Sub-Committee (WWNWS-SC) has formed an EGC-API Correspondence Group (EGC-API CG) to develop an application programming interface (API) standard to support the machine-to-machine transfer of Enhanced Group Call (EGC) shore-to-ship information between certified and registered Maritime Safety Information Providers (MSIP) and Recognized Mobile Satellite Service (RMSS) providers.

Abbreviations/Glossary

IA5	International Alphabet No.5 (IA5) is character encoding defined in ITU-T Recommendation T.50[1]
API	application programming interface
EGC	enhanced group call
MSI	maritime safety information
MSIP	maritime safety information provider
RMSS	recognized mobile satellite service

Procedure

In accordance with paragraph **3.c.** of the EGC-API CG Terms of Reference, the EGC-API CG will:

> *identify desirable requirements in support of **3.b.***

that states, the EGC-API CG will:

> *review the needs and requirements for an EGC-API standard to support the machine-to-machine transfer of EGC shore-to-ship information between certified and registered [MSI] providers and recognized mobile-satellite service providers.*

This document contain the desirable requirements of the standard, as agreed by the EGC-API CG.

[1] Also referred to as the International Reference Alphabet (IRA) or ASCII extended

Desirable requirements

Requirement No 1: The API should allow for the creation of one or more messages in an authenticated session.

Requirement No 2: The API should return a timestamp in an ISO 8601 format, generated by the RMSS system.

Requirement No 3: The API should allow an MSIP to provide a self-generated unique identification (SGID) for reference to a new message.

Requirement No 4: The API should return a unique identification (ID) generated by the RMSS system when a new and valid message is submitted by the MSIP.

Requirement No 5: The API should return an error code when the RMSS system identifies an error in a new message submitted by the MSIP.

Requirement No 6: The API should return the status of a message, generated by the RMSS system, when the MSIP requests it by supplying the ID.

Requirement No 7: The API should return the status and ID of all in-force messages, generated by the RMSS system, when the MSIP requests it.

Requirement No 8: The API should allow a message to be cancelled (removed from the automatic broadcast schedule) when the MSIP requests it by supplying the ID.

Requirement No 1

The API should allow for the creation of one or more messages in an authenticated session.

This requirement is to streamline authentication and not to provide a batch submission method.

When the MSIP is authenticated with the RMSS system, for the duration of the session, the API will permit a new message to be uploaded when:

- the previous message is validated and a unique identification (ID) has been returned (refer to Requirement No 4); or
- the RMSS system identifies an error in the previous message submitted by the MSIP and returns an error code (refer to Requirement No 5).

Requirement No 2

The API should return a timestamp in an ISO 8601 format, generated by the RMSS system.

When an MSIP makes a call to the API, a timestamp should be returned in an ISO 8601 format. Timestamp validity, as determined by the RMSS system, should be detailed in the RMSS documentation.

Requirement No 3

The API should allow an MSIP to provide a self-generated unique identification (SGID) for reference to a new message.

RMSS providers should document if an MSIP can provide a self-generated unique identification (SGID) in a call to the API and its functionality. If the API supports a SGID, then a call to the API with a SGID should return the SGID with an ID, status or error code (refer to Requirement Nos 4, 5 and 6).

Requirement No 4

The API should return a unique identification (ID) generated by the RMSS system when a new and valid message is submitted by the MSIP.

This is a unique identification (ID) generated by the RMSS system for each new message as required by IMO resolution A.1001(25) and MSC.1/Circ.1364/Rev.1. The ID should be traceable and used as a reference to messages in the RMSS system when making a call to the API (e.g. to check the status).

Note: For Iridium SafetyCAST, this is the “Advisory_ID”. For Inmarsat SafetyNET II and RescueNET, this is the “Reference Number”.

Requirement No 5

The API should return an error code when the RMSS system identifies an error in a new message submitted by the MSIP.

When an MSIP submits a new message via a call to the API, if the RMSS system identifies an error, the API should return an error code. This may include:

- invalid payload (e.g. invalid IA5 character encoding)
- invalid C code request (e.g. action not defined by C codes in the Inmarsat SafetyNET II, RescueNET or Iridium SafetyCAST Manuals)

When an error code is returned by the API, a unique identification (ID) should not be returned.

In the RMSS documentation, providers should identify what error codes (and the checks the RMSS system is performing) the API will return.

Note: It is a responsibility of MSIP to ensure the payload and C code request is valid.

Requirement No 6

The API should return the status of a message, generated by the RMSS system, when the MSIP requests it by supplying the ID.

In the RMSS documentation, providers should identify what statuses its API will return and for how long (after creation or cancellation of a message) an MSIP can query the status of a message.

Requirement No 7

The API should return the status and ID of all in-force messages, generated by the RMSS system, when the MSIP requests it.

When an MSIP requests via a call to the API, the RMSS system will return the status and ID of all in-force messages. In the RMSS documentation, providers should identify the format that this request will be returned.

Requirement No 8

The API should allow a message to be cancelled (removed from the automatic broadcast schedule) when the MSIP requests it by supplying the ID.

This function cannot be achieved through C codes and is a direct instruction to the RMSS provider that will remove an existing message from the automatic broadcast schedule.

Note: It is a responsibility of MSIP to ensure a new self-cancelling message is broadcast to advise an existing message has been cancelled.