

RECOMMENDATION (NORMATIVE)

RNNNN VDE PAYLOAD FORMAT IDENTIFIERS (VPFI)

Edition 1.0

June 2026

urn:mrn:iala:pub:rnnnn:ed1.0



DOCUMENT REVISION

Revisions to this document are to be noted in the table prior to the issue of a revised document. The latest edition of the Recommendation is the only version in force unless the Recommendation is explicitly revoked by the Council.

Date	Revision details	Approval
June 2026	Edition 1.0	Council 04

THE COUNCIL

RECALLING

- 1 The aim and objectives of the International Organization for Marine Aids to Navigation (the Organization) with respect to the improvement and harmonization of Marine Aids to Navigation (AtoN) worldwide for the benefit of the maritime community and the protection of the marine environment;
- 2 Article 8 of the Convention of the Organization regarding the responsibilities of the Council;

RECALLING FURTHER

- 1 The work of the Organization in defining and implementing the Automatic Identification System (AIS);
- 2 That the VHF Data Exchange System (VDES) includes functions for AIS, Application Specific Messages (ASM), and VHF Data Exchange (VDE-TER and VDE-SAT);
- 1 That the VDES is coordinated by the Organization in consultation with the International Telecommunication Union (ITU), the International Maritime Organization (IMO), and the International Electrotechnical Commission (IEC);

RECOGNIZING the need of a harmonized way to indicate to the maritime applications the data format used inside VDE data packets to enable applications to use the data;

INVITING Members of the Organization and sister organizations that are involved in VDE application design to engage further in developing guidance on the subject;

HAVING CONSIDERED the proposals made by the Digital Technologies Committee;

APPROVES Recommendation RNNNN on VDE Payload Format Identifiers, set out in the Annex;

INVITES Members of the Organization and AtoN authorities and other appropriate stakeholders worldwide to implement the provisions of this Recommendation;

REQUESTS the Digital Technologies Committee or other Committees as the Council may direct, to keep this Recommendation under review and to propose amendments as necessary.

ANNEX VDE PAYLOAD FORMAT IDENTIFIERS

- 1 The VDE Payload Format Identifiers (VPFI) have the purpose to allow VDE applications to uniquely identify how to interpret the digital content of VDE messages.
- 2 To ensure global interoperability, the Organization maintains a harmonized registry of VPFI numbers and their associated data formats. This registry serves as the definitive technical reference for VDE application developers and system integrators.
- 3 Members of the Organization and AtoN authorities and other appropriate stakeholders should comply with the requirements for the VPFI allocation requirements and technical specifications as set out in the Appendix.

APPENDIX 1 UNIQUE IDENTIFIER FOR VDE PAYLOAD FORMATS

1 CONTEXT

Guideline G1117 Edition 3.0 has captured the initial VDE Payload Format Identifiers (VPFI) concept and listed several formats. As of 2026, the IEC adopted the concept for the VPFI in its draft IEC 63514 standard on "requirements and test methods for shipborne mobile VDES station".

Furthermore, RTCM adopted the concept for the VPFI in Annex C and D of its RTCM Standard 13900.0 for Maritime Messaging Service Architecture and Protocol.

These adoptions can be expected to be the start of a widespread use of the VPFI as a harmonized identification concept for VDE data payload formats, and therefore, a dedicated guideline is indicated.

2 DEFINITIONS

This section contains any core terms and definitions considered important to assist in the understanding of the document content. Other terms and definitions can be found in the International Dictionary of Marine Aids to Navigation of the Organization.

2.1 FIELD FORMATS

BYTE8-bit field

BYTE[n]n*8-bit field

BYTE[]variable-size field

WORD16-bit field

DWORD32-bit field

Byte ordering inside multi-byte fields is according to ITU-R M.2092 Technical characteristics for VHF data exchange system in the maritime mobile service.

2.2 VDES EQUIPMENT

VDES Equipment may be VDES shore base stations, VDES mobile stations, or any other fixed or mobile VDES-based transceiver stations operating according to ITU-R M.2092.

2.3 VDE APPLICATION

An application that uses methods of transport defined in ITU-R M.2092-2, Annex 3, 4, or 5 for ASM, VDE-TER, or VDE-SAT, respectively.

3 CONCEPT

The VPFI is a unique number in the range from 0 to 268,435,455 that uniquely and globally identifies the specific protocol or data format for the digital content that follows the VPFI in the data that is received or sent via ASM, VDE-TER or VDE-SAT.

This Recommendation identifies a given identifier number and the associated application guideline or reference using that VPFI.

Table 1- Variable size of the VPFI in VDE Data; shown are examples with 1, 2, or 3 bytes of VPFI; more bytes can be used, the concept stays the same.

Byte	1-Byte VPFI	2- byte VPFI	3-byte VPFI	4-byte VPFI
1	VDE Payload Format Identifier (VPFI)	VDE Payload Format Identifier (VPFI)	VDE Payload Format Identifier (VPFI)	VDE Payload Format Identifier (VPFI)
2	VDE Application Data			
3		VDE Application Data		
4			VDE Application Data	
5 ...				VDE Application Data

3.1 VDE PAYLOAD FORMAT IDENTIFIERS

The different bytes in a VPFI are identified as Levels.

As indicated in **Erreur ! Source du renvoi introuvable.**,

A 1-byte “Level 1” VPFI provides room to distinguish 128 payload formats.

A 2-byte “Level 2” VPFI provides room to distinguish $128^2 = 16,384$ payload formats.

A 3-byte “Level 3” VPFI provides room to distinguish $128^3 = 2,097,152$ payload formats.

A 4-byte “Level 4” VPFI provides room to distinguish $128^4 = 268,435,456$ payload formats.

Less widely used payload formats should use Level 2 VPFI.

3.1.1 LEVEL 1

The first byte of the VPFI identifies:

- If there follows another byte to extend the VPFI range, and
- applications that only require 1 byte of overhead to be indicated.

Table 2- Level 1 VPFI allocations

VPFI Byte 1 content	Application Name	Reference/Note
0	VDES mobile station payload formats	See IEC 63514 §4.1 and relevant IEC documents
1	VDES Management Messages	See §4.2
2	VDE Text Messages	See §4.3
3	GNSS Augmentation	See §4.4
4	Maritime Messaging Service	RTCM 13900.0 Maritime Messaging Service Architecture and Protocol.
5	Regional Applications	See §4.6
6	(not allocated)	Reserved for future use.
7	Authentication	See §4.7
8..126	(not allocated)	Reserved for future use.
127	For test purposes	Do not use for operational services.

VPFI Byte 1 content	Application Name	Reference/Note
128-255	Indicates that next byte also is part of VPFI.	See next chapter on “Level 2”.

3.1.2 LEVEL 2

An optional 2nd byte identifies:

- If there follows another byte to extend the VPFI range, and
- The 7 least significant bits of the application identifier, that with the 7 bits of the first byte give space for $2^{14}-1 = 16\,383$ payload format identifiers.

Table 3 - Level 2 VPFI allocations

VPFI Byte 1 content	VPFI Byte 2 content	Application Name	Reference
128	0	<application 1 of Level 2>	Reserved for future use.
128	1	<application 2 of Level 2>	
...	
128	127	<application 128 of Level 2>	
129	0	<application 129 of Level 2>	
129	1	<application 130 of Level 2>	
...	
129	127	<application 256 of Level 2>	
...	...		
255	126	<application 16,383 of Level 2>	
255	127	For test purposes	No coordination of the format.
128-255	128-255	Indicates that next byte also is part of VPFI.	See next chapter on “Level N”.

3.1.3 LEVEL 3 AND 4

After the 2nd byte, more bytes can be added to the VPFI if a greater application range is needed in the future. Each added byte creates a new level with 128^n more applications to be fit.

4 VDE PAYLOAD FORMATS

This section lists all VPFI messages coordinated with IALA DTEC.

In order to allow the receiver of VPFI messages to check for identity and integrity of the data received, all VPFI messages should be requested to be authenticated by the VDES Equipment when transferred to the VDES Equipment, as described in detail in ITU-R M.2092.

4.1 VPFI 0: IEC: VDES MOBILE APPLICATIONS

This section lists VPFI 0 messages for the use in the VDES mobile station.

The message formats for VPFI 0 messages are listed in Table 4.

Table 4 - VDES Mobile VPFI 0 Message formats

Message format	Description
0	Certificate Request
1	Certificate Report
2	Encapsulated AIS Message
3	UTF8 Text Message
4	Application Acknowledgement
5	VDE-TER Status Report
6	Encapsulated ASM Message
7	VDE AtoN Report

4.1.1 CERTIFICATE REQUEST

Used to request a certificate.

Table 5 - Certificate Request

Field	Type	Description
VPFI	BYTE	VDE Payload Format Identifier. Shall be set to 0.
Message format	BYTE	Indicating Certificate Request. See Table 4.
Certificate fingerprint	BYTE[6]	Fingerprint of the requested certificate. This parameter can be left empty (zero number of bits) to indicate that receiver should respond with own public certificate that can be used to authenticate the receiver.

4.1.2 CERTIFICATE REPORT

This report should be used to broadcast one or more X.509 public key certificates and/or one or more certificate revocation lists (CRL) that could be used for authentication. This report is either sent on request for a specific certificate, or it may be sent without a request. When multiple certificates are reported in the chain of trust, the certificates should be ordered from highest to lowest level, first to last in the report.

A root certificate should not be transmitted in a certificate report.

A certificate is requested using a fingerprint as identification, however multiple certificates might match the fingerprint. In this case the report might also contain multiple certificates with the same fingerprint.

Table 6 - Certificate Report

Field	Type	Description
VPFI	BYTE	VDE Payload Format Identifier. Shall be set to 0.
Message format	BYTE	Indicating Certificate Report. See Table 4.
Number of Certificates in report (n)	BYTE	The number of certificates and CRLs included in the report.

Field	Type	Description
Issuer certificate fingerprint[0]	BYTE[6]	Fingerprint of certificate of the CA that issued the certificate in the following field. The issuer certificate must be authenticated before the received certificate can be authenticated.
Certificate type[0]	BYTE	0: Intermediate /End certificate 1: Root-issued Intermediate certificate 2: Certificate revocation list 3-255: Reserved for future use
Certificate Length[0]	WORD	The number of bytes to follow in Certificate field.
Certificate[0]	BYTE[]	Array of bytes. Certificate (version 3) encoded in DER format as referenced in ITU-T X.509.
...
Issuer certificate fingerprint[n-1]	BYTE[6]	
Certificate type[n-1]	BYTE	
Certificate Length[n-1]	WORD	
Certificate[n-1]	BYTE[]	

4.1.3 ENCAPSULATED AIS MESSAGE

This message is used to encapsulate one or multiple AIS messages as defined in ITU-R M.1371.

Table 7 – Encapsulated AIS Message

Field	Type	Description
VPFI	BYTE	VDE Payload Format Identifier. Shall be set to 0
Message format	BYTE	Indicating VPFI encapsulating AIS messages. See Table 4.
Number of AIS Messages (n)	BYTE	The number of AIS messages in this message.
Length of AIS message 0	WORD	Length of the first AIS message in bits.
AIS message 0	BYTE[]	AIS message data as defined in ITU-R M.1371.
...
Length of AIS message n-1	WORD	Length of the nth AIS message in bits.
AIS message n-1	BYTE[]	AIS message data as defined in ITU-R M.1371.

4.1.4 UTF8 TEXT MESSAGE

This message is used to send text messages using UTF8 encoding.

Table 8 – UTF8 Text Message

Field	Type	Description
VPFI	BYTE	VDE Payload Format Identifier. Shall be set to 0.
Message format	BYTE	Indicating UTF8 Text Message. See Table 4.
Acknowledge required	WORD	Uses the most significant bit (bit 15) of this field. The value should be ignored if broadcast addressing has been used. 0: Reply is not required. 1: Reply is required. Addressed receiver must respond with Application Acknowledgement Message.
Sequence number		Uses bits 14:0 of this field. 0 – 2 ¹⁵ -1: Unique sequence number identifying this message.
Text string	BYTE[]	UTF-8 encoded text (see ISO/IEC 10646:2021).

4.1.5 APPLICATION ACKNOWLEDGEMENT MESSAGE

This message is used to acknowledge a VPFI message.

Table 9 – Application Acknowledgement Message

Field	Type	Description
VPFI	BYTE	VDE Payload Format Identifier. Shall be set to 0.
Message format	BYTE	Indicating Application Acknowledgement Message. See Table 4.
VPFI Being Acknowledged	BYTE	VPFI:Message ID pair being acknowledged.
Message ID Being Acknowledged	BYTE	
Sequence number	WORD	Sequence number from received message that is being acknowledged.

4.1.6 VDE-TER STATUS REPORT

This message is used to report VDE-TER Status information.

Table 10 VDE-TER Status Report

Field	Type	Description
VPFI	BYTE	VDE Payload Format Identifier. Shall be set to 0.
Message format	BYTE	Indicating VDE-TER Status Report. See Table 4.
MMSI of TBB in use	DWORD	MMSI of TBB that is currently in use by reporting station. Set to 0 if default TBB is in use.
Priority	BYTE	Service area priority level field value from TBB in use.
Bulletin board version	WORD	Version number of TBB in use.
Capability	BYTE	Specifies the capabilities of the equipment. 0: Equipment complies to edition 1 of IEC 63514.

Field	Type	Description
		1-255: Reserved for future use.
Number of VDE-TER receivers	BYTE	The number of VDE-TER receivers supported.
Number of VDE-SAT receivers	BYTE	The number of VDE-SAT receivers supported.
Link IDs supported	WORD	Each set bit value indicates if the receivers support a specific Link ID. Bit 0: Link ID 12 Bit 1: Link ID 13 Bit 2: Link ID 14 Bit 3: Link ID 15 Bit 4: Link ID 16 Bit 5: Link ID 18 Bit 6: Link ID 23 Bit 7: Link ID 27 Bit 8: Link ID 28 Bit 9: Link ID 29 Bit 10: Link ID 35 Bit 11: Link ID 36 Bit 12: Link ID 37 Bit 13: Link ID 38 Bit 14: Link ID 41 Bit 15: Link ID 42 Bit 16: Link ID 48

4.1.7 ENCAPSULATED ASM MESSAGE

This message is used to encapsulate AIS ASM binary data formatted as defined in ITU-R M.1371 for transmission over VDE VDL. For example, to transport the ASMs defined by IMO in SN.1/Circ.289.

Table 11 Encapsulated ASM Message

Field	Type	Description
VPFI	BYTE	VDE Payload Format Identifier. Shall be set to 0.
Message format	BYTE	Indicating ASM Message. See Table 4.
Number of ASM Messages (n)	BYTE	Number of encapsulated ASMs.
Length of ASM message 0	WORD	Number of bits in ASM message 0.
ASM message 0 (first ASM)	BYTE[]	ASM binary data as defined in ITU-R M.1371.
...
Length of ASM n-1	WORD	Number of bits in ASM message n-1.
ASM message n-1 (last ASM)	BYTE[]	ASM binary data as defined in ITU-R M.1371.

4.1.8 VDE AtoN REPORT

This message is used to distribute one or multiple AIS AtoN Reports (AIS VDL Message 21) to be output on the PI using VDM sentences as defined in IEC 61162.

Table 12 VDE AtoN report

Field	Type	Description
VPFI	BYTE	VDE Payload Format Identifier. Shall be set to 0.
Message format	BYTE	Indicating Virtual AtoN Message. See Table 4.
Number of AtoN Reports (n)	BYTE	Number of AtoN Reports.
Length of AtoN Report 0	BYTE	Number of bytes in AtoN Report 0, counted from Virtual AtoN flag 0 to Name of Aids-to-Navigation 0.
Virtual AtoN flag 0	DWORD	Bit 31 of DWORD. 0 = default = physical AtoN at indicated position; 1 = virtual AtoN, does not physically exist.
Validity 0		Bit 30 of DWORD. 0: Valid. 1: AtoN information is no longer valid.
Source ID 0		Bits 29:0 of DWORD. Identity of the virtual AtoN station. See Article 19 of the RR and Recommendation ITU-R M.585.
Type of Aids-to-Navigation 0	BYTE	Used to populate AIS Message 21 Type of aids-to-navigation field. See ITU-R M.1371-6 Table 71. Only the least-significant 5 bits are used.
Longitude 0	DWORD	Used to populate AIS Message 21 Longitude field. See ITU-R M.1371-6 Table 71. Only the least-significant 28 bits are used.
Latitude 0	DWORD	Used to populate AIS Message 21 Latitude field. See ITU-R M.1371-6 Table 71. Only the least significant 27 bits are used.
AtoN status 0	BYTE	Used to populate AIS Message 21 AtoN status field. See ITU-R M.1371-6 Table 71.
Name of Aids-to-Navigation 0	BYTE[]	Used to populate AIS Message 21 Name of Aid-to-Navigation and Name of Aids-to-Navigation Extension field. See ITU-R M.1371-6 Table 71. Only the first multiple-of-six bits of this field is used. If the number of bits is not a multiple of six, then the least-significant bits in the last byte is not used.
...
Length of AtoN Report n-1	BYTE	Number of bytes in AtoN Report n-1, counted from Virtual AtoN flag n-1 to Name of Aids-to-Navigation n-1.
Virtual AtoN flag n-1	DWORD	Bit 31 of DWORD. 0 = default = physical AtoN at indicated position; 1 = virtual AtoN, does not physically exist.
Validity n-1		Bit 30 of DWORD.

Field	Type	Description
		0: Valid. 1: AtoN information is no longer valid.
Source ID n-1		Bits 29:0 of DWORD. Identity of the virtual AtoN station. See Article 19 of the RR and Recommendation ITU-R M.585.
Type of Aids-to-Navigation n-1	BYTE	Used to populate AIS Message 21 Type of aids-to-navigation field. See ITU-R M.1371-6 Table 71. Only the least-significant 5 bits are used.
Longitude n-1	DWORD	Used to populate AIS Message 21 Longitude field. See ITU-R M.1371-6 Table 71. Only the least-significant 28 bits are used.
Latitude n-1	DWORD	Used to populate AIS Message 21 Latitude field. See ITU-R M.1371-6 Table 71. Only the least significant 27 bits are used.
AtoN status n-1	BYTE	Used to populate AIS Message 21 AtoN status field. See ITU-R M.1371-6 Table 71.
Name of Aids-to-Navigation n-1	BYTE[]	Used to populate AIS Message 21 Name of Aid-to-Navigation and Name of Aids-to-Navigation Extension field. See ITU-R M.1371-6 Table 71. Only the first multiple-of-six bits of this field is used. If the number of bits is not a multiple of six, then the least-significant bits in the last byte is not used.

4.2 VPFI 1: VDES MANAGEMENT MESSAGES

The message formats for VPFI 1 messages are listed in Table 13.

Table 13 - VPFI 1 Message formats

Message format	Description
0	VDE-SAT Network Orbit Data
1-255	Reserved for future applications.

4.2.1 VDE-SAT NETWORK ORBIT DATA

This message is used to inform about updated orbital data for a set of VDE-SAT satellites in a VDE-SAT network or VDE-SAT roaming network. Equipment may use the orbital data to estimate when connectivity to a satellite can be expected.

Orbital data is represented in the two-line element (TLE) format.

Table 14 - VDE-SAT Network Orbit Data

Field	Type	Description
VPFI	BYTE	VDE Payload Format Identifier. Shall be set to 1.
Message format	BYTE	Indicating VDE-SAT Network Orbit Data, see Table 13 - VPFI 1 Message formatsTable 13.

Primary network ID	BYTE	Values 0-255 allowed, see ITU-R M.2092-1, Annex 5, §3.1.9
Roaming network ID	BYTE	Identifying which roaming network group the satellites of this list belong to.
n	BYTE	Number of orbital data sets transferred in this VDE Payload Format
Satellite ID[0]	BYTE	ID [0] of the satellite
TLE [0]	BYTE[10 4]	TLE data[0] for the first satellite: 2 lines of 69 ASCII 6-bit encoded characters, followed by 4 padding bits.
Satellite ID[1]	BYTE	ID [1] of the satellite
TLE [1]	BYTE[10 4]	TLE data[1] for the second satellite: 2 lines of 69 ASCII 6-bit encoded characters, followed by 4 padding bits.
...
Satellite ID[n-1]	BYTE	ID [n-1] of the satellite
TLE [n-1]	BYTE[10 4]	TLE data[n-1] for the nth satellite: 2 lines of 69 ASCII 6-bit encoded characters, followed by 4 padding bits.

4.3 VPFI 2: VDE TEXT MESSAGES

The message formats for VPFI 2 messages are listed in Table 15

Table 15 - VPFI 2 Message formats

Message format	Description
0	Text using UTF-8 encoding, encrypted
1..255	Reserved for future applications

4.3.1 EXT USING UTF-8 ENCODING, ENCRYPTED

This message is used to send encrypted text messages using UTF8 encoding.

Encryption is applied only to the text string field, using the public key of the receiver, according to IEC 63173-2:2022, 7.6.2 Encryption Algorithm.

Table 16 – UTF8 encrypted Text Message

Field	Type	Description
VPFI	BYTE	VDE Payload Format Identifier. Shall be set to 2.
Message format	BYTE	Indicating UTF8 encrypted Text Message. See Table 15.
Acknowledge required	WORD	Uses most significant bit (bit 15) in this field. Value should be ignored if broadcast addressing has been used. 0: Reply is not required. 1: Reply is required. Addressed receiver must respond with Application Acknowledgement Message.
Sequence number		Uses Bits 14:0 in this field. 0 – 2 ¹⁵ -1: Unique sequence number identifying this message.
Text string	BYTE[]	UTF-8 encoded text (see ISO/IEC 10646:2021) as output by the encryption algorithm.

4.4 VPFI 3: GNSS AUGMENTATION

This message is used to transfer GNSS augmentation data, e.g. like described in Guideline G1117.

Table 17 - GNSS augmentation data over VDE-TER and/or VDE-SAT

Field	Type	Description
VPFI	BYTE	VDE Payload Format Identifier. Shall be set to 3.
Augmentation Type	BYTE	0 = SBAS corrections & integrity in RTCA format 1 = SBAS corrections & integrity in RTCM format 2 = RTK corrections in SSR format 3 = PPP corrections in SSR format 4 = RTK corrections in RTCM OSR format. 5..255 = Reserved for future use
Augmentation data	BYTE[]	Data is packed as per the transport layer definition according to the augmentation type.

4.5 VPFI 4: MARITIME MESSAGING TRANSFER PROTOCOL (MMTP) MESSAGE

This message is used to indicate an encapsulated MMTP message, which use is defined in the RTCM Maritime Messaging Service and Protocol Specification 13900.0.

Table 18 - VPFI 4: MMTP

Field	Format	Description
VPFI	BYTE	VDE Payload Format Identifier. Shall be set to 4.
MMS Data	BYTE[]	See RTCM 13900.0

4.6 VPFI 5: REGIONAL APPLICATIONS

This message is used to transfer regional application data.

Table 19 – Regional Application Data

Field	Type	Description
VPFI	BYTE	VDE Payload Format Identifier. Shall be set to 5.
Region Identifier	WORD	Bits 15..6: Encoded as the designated area code (DAC), see ITU-R M.1371. Bits 5..0: regionally defined, default = 0.
Regional Application Data	BYTE[]	Regional Application data of regional application.

4.7 VPFI 7: AUTHENTICATION

This VPFI is used for messages that provide authentication of data transmitted over VDES. Messages using this VPFI carry data required to verify the authenticity and integrity of transmissions, and to confirm that those transmissions have not been replayed.

The application of these messages within specific authentication schemes – including the operational procedures for message generation, transmission, reception and verification – is described in *Guideline G1192 VDES Authentication Techniques*.

Table 20 Message types for VPFI=7

Message format	Description
1	Signature Message for VDES Authentication Scheme 1
0, 2–63	Reserved for future use.

4.7.1 SIGNATURE MESSAGE FOR VDES AUTHENTICATION SCHEME 1

This message carries the digital signature and associated metadata required to authenticate an AIS message transmitted on the AIS channels.

Note: This message provides authentication in an integrated manner and therefore, VDES Signed Segments authentication as defined in ITU-R M.2092-2 should not be used.

Table 21: Signature Message for VDES Authentication Scheme 1

Field No.	Parameter	Bitcount	Decimal Value	Description
1	VPFI	16	7	VDE Payload Format Identifier. Shall be set to 7, indicating 'Cryptographic Authentication'. See IALA G1117 for further details on the VPFI concept.
2	Message format	6	1	Allows for multiple message formats to be used within a given authentication scheme.
3	Authentication Scheme ID	8	1	Identification of the authentication scheme being used. Shall be set to 1, indicating 'AIS Message Authentication over VDE-TER'. Provides flexibility for future revisions to address evolving security requirements.
4	AIS Message ID	6	1 to 63	The Message ID of the AIS message being signed.
5	MMSI	30	0 to 230-1	The Maritime Mobile Service Identity of the sender of the AIS message being signed. Refer to Rec. ITU-R M.1371.
6	Channel ID	2	0 to 3	The channel where the AIS message being signed was transmitted. 0: AIS1

Field No.	Parameter	Bitcount	Decimal Value	Description
				1: AIS2 2-3: Reserved for future use
7	Slot number	12	0 to 2249	The number of the slot in which the AIS message being signed was transmitted, as defined in Rec. ITU-R M.1371. Note: AIS base stations can output the slot number in the VSI PI sentence.
8	Timestamp	32	0 to 232-1	Time when the AIS message being signed was transmitted on the VHF Data Link (VDL). Unsigned integer number of seconds after 1st January 1970 00:00:00 UTC. If the recipient determines that the Timestamp is more than 60 seconds before the time of receipt of this Signature Message then this Signature Message shall be discarded.
9	Certificate Fingerprint	48	0 to 248-1	A fingerprint identifying the public key certificate to be used to verify the digital signature in field 10 of this message. The fingerprint is taken as the 48 least significant bits of the certificate's signatureValue (see RFC 5280, Section 4.1.1.3).
10	Signature	512	0 to 2512-1	A digital signature calculated over the concatenation of fields 1-9 of this message and the bit structure of the AIS message being signed, as defined in Rec. ITU-R M.1371. The bits corresponding to the AIS message shall form the least significant bits of the concatenated data. The signature algorithm is defined in G1192.
-	Total bitcount	672	-	-

5 ABBREVIATIONS

AIS	Automatic Identification System acc. to ITU-R M.1371
AIS-ASM	An ASM transmitted over AIS acc. to ITU-R M.1371-6
ASM	Application Specific Message
PI	VDES Presentation Interface, see ITU-R M.2092
VDE	VHF Data Exchange, may be terrestrial (VDE-TER) or satellite (VDE-SAT)
VDES	VHF Data Exchange System
VDES-ASM	An ASM transmitted over the ASM channels acc. to ITU-R M.2092
VPFI	VHF Data Exchange Payload Format Identifier
VPFI Message	A message format that is identified by the VPFI