IALA GUIDELINE

GNNNN
VDES AUTHENTICATION TECHNIQUES

Edition 1.0

June 2025

urn:mrn:iala:pub:gnnnn:ed.1.0

10, rue des Gaudines - 78100 Saint Germain en Laye, France
Tel. +33 (0)1 34 51 70 01 - contact@iala.int
www.iala.int
International Organization for Marine Aids to Navigation

DOCUMENT REVISION

Revisions to this document are to be noted in the table prior to the issue of a revised document.

Date	Details	Approval
June 2025	First edition	Council 02

CONTENTS

CONTENTS

CONTENTS

List of Tables

List of Figures

1. INTRODUCTION

The maritime industry is undergoing a digital transformation, bringing with it new opportunities to enhance safety, efficiency and sustainability at sea. At the heart of these developments is the Very High Frequency (VHF) Data Exchange System (VDES) [1], a next-generation communication system that includes and extends the capabilities of the Automatic Identification System (AIS) and supports the International Maritime Organisation's (IMO) e-navigation initiative [2]. VDES offers a harmonised global platform for maritime data exchange, representing a key enabler of the digital maritime future.

As data exchange becomes central to maritime operations and technical barriers to radio spectrum access diminish, there is a growing need for *data authentication* - the ability to confirm that data originates from a trusted source and has not undergone unauthorised modification. Unlike the existing AIS, which lacks built-in mechanisms to verify data authenticity, VDES offers a unique opportunity to incorporate cryptographic authentication into the system's design and operation from the outset.

This guideline marks a significant step forward in realising that potential. By providing clear, implementable approaches to authenticating data transmitted over VDES, it supports the development of a more secure and resilient maritime communication environment. This document not only addresses urgent cybersecurity needs but also demonstrates IALA's commitment to proactive leadership in shaping the future of trusted maritime communication.

1.1. PURPOSE OF THIS GUIDELINE

The purpose of this guideline is to identify and promote cryptographic authentication techniques that are suitable for use with VDES. Through careful analysis and practical examples, it provides a solid foundation for improving the trustworthiness of maritime data transmission.

This is the first IALA document to offer a detailed, implementable solution for AIS message authentication using VDES. The guideline will support competent authorities and industry stakeholders in addressing the cybersecurity recommendations set out in IALA R1007 *The VHF Data Exchange System (VDES) for Shore Infrastructure* and R1024 *Cyber Security for the IALA Domains*.

1.2. SCOPE

The first edition of this guideline concentrates on the authentication of high-priority, safety-critical messages, such as Virtual AIS Aids to Navigation (AtoN) reports. By focusing on these relatively infrequent but operationally important transmissions, the guideline demonstrates that robust authentication can be achieved with minimal impact on the VDES data link, setting a clear path for future editions to address additional applications.

The topics covered in this guideline include:

- The importance of authentication in AIS and VDES communications.
- Fundamental concepts in cryptographic authentication, including symmetric and asymmetric (public key) cryptography, digital signatures and public key infrastructure (PKI).
- Technical and operational challenges in implementing VDES authentication, such as maintaining backwards compatibility with legacy AIS systems and operating within the data rate constraints of VDES.
- Authentication requirements derived from specific e-navigation applications and use cases.
- Detailed proposals for implementing cryptographic authentication solutions, including their expected impact on VDES data link loading.

- Recommendations for future work, standardisation pathways and research directions to support the development of a robust VDES authentication framework.

The following topics are considered outside the scope of this document, but references to complementary work are provided where appropriate:

- Mitigation of vulnerabilities in Global Navigation Satellite Systems (GNSS), such as spoofing of positioning and timing signals.
- Encryption of messages or other approaches to keep user data secret.
- The establishment of a maritime PKI.

2. VDES OVERVIEW

2.1. SYSTEM CONTEXT

2.1.1. E-NAVIGATION SYSTEM OF SYSTEMS

VDES can be considered as part of a broader e-Navigation system of systems (SoS), a globally coordinated framework designed to enhance the safety, security, efficiency and environmental sustainability of maritime operations. This system comprises an array of interconnected systems and digital services, all functioning together to support a wide range of maritime use cases.

Among these systems are digital maritime service platforms – such as the Maritime Connectivity Platform (MCP) – resilient positioning, navigation and timing (PNT) solutions and visual Aids to Navigation (AtoN). These interconnected elements contribute to the delivery of harmonised information and services to mariners and shore-based operators.

The context diagram in Figure 1 illustrates the interactions between the e-Navigation SoS, its users and the VHF radio environment.

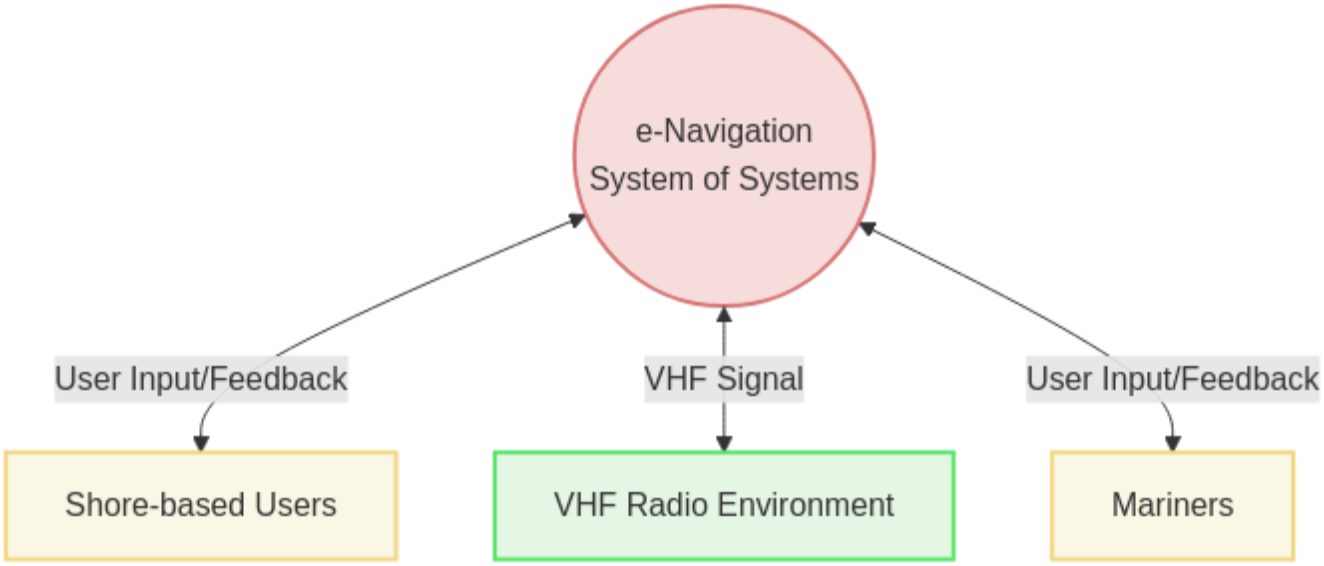

Figure 1 E-Navigation system of systems context diagram

2.1.2. VDES CONTEXT

Zooming in on the role of VDES within this broader framework, Figure 2 presents the specific context in which VDES operates. It illustrates how VDES interacts with its users, depicted in yellow, and its integration with various external systems, shown in blue.

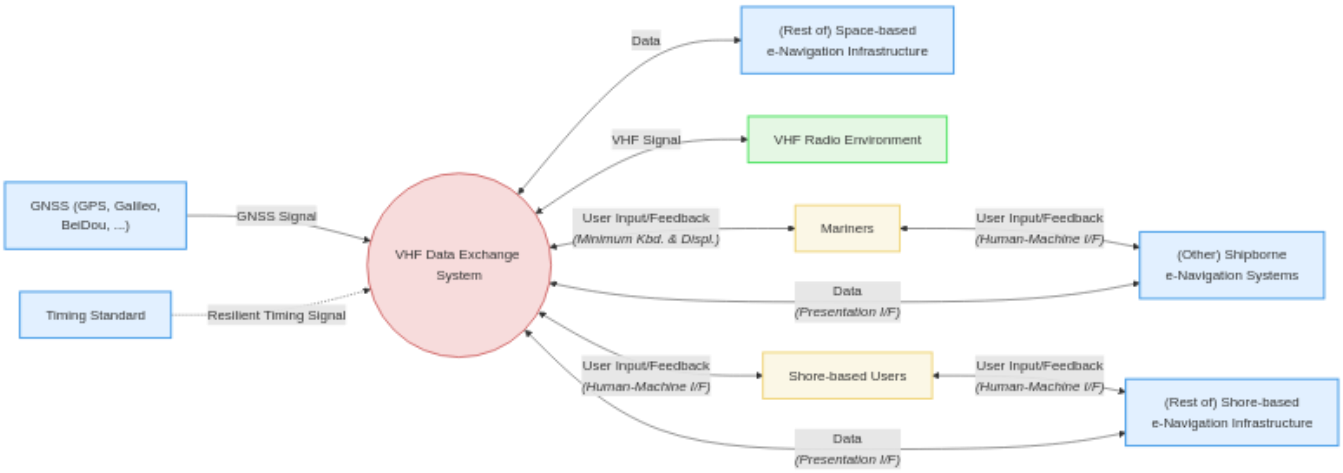

Figure 2 VDES context diagram

2.1.2.1. Shipborne Integration

Onboard vessels, mariners can interact with VDES through a Minimum Keyboard and Display (MKD) for direct input (e.g. updating voyage information). More commonly, however, VDES integrates with an Electronic Chart Display and Information System (ECDIS), radar, and other shipborne e-Navigation systems via a machine-to-machine data interface known as the Presentation Interface (PI).

2.1.2.2. Shore-based Systems

System operators ashore will be provided with basic user interfaces for configuration and monitoring of terrestrial VDES equipment. These are likely to be manufacturer specific. The VDES equipment will integrate into a broader shore-based e-Navigation infrastructure via the Presentation Interface. Users on land will then primarily interact with VDES through higher-level applications and services provided by this infrastructure.

2.1.2.3. Space Segment

In parallel with terrestrial communications, VDES supports two-way data flows between terrestrial stations and space-based assets. This will again likely be through the Presentation Interface, with the space-based e-Navigation infrastructure acting as a relay for data between land-based and shipborne stations worldwide.

2.1.2.4. Supporting Infrastructure

Global Navigation Satellite Systems (GNSS) provide the precise positioning and timing required for VDES operation. For resilience, additional timing signals may be provided (e.g. via eLoran, fibre-optic links or an atomic clock) to ensure continued operation when GNSS signals are disrupted.

2.2. SYSTEM ARCHITECTURE

2.2.1. OVERVIEW

VDES is designed to augment and protect AIS functions while providing significantly higher data throughput and improved reliability for general data exchange with global coverage. It can be divided into four main functional components, each using different radio channels, waveforms and protocols, optimised for different applications and use cases. These are:

1. The original AIS;
2. VDES Application Specific Messaging (VDES ASM);
3. Terrestrial VHF Data Exchange (VDE-TER); and
4. Satellite VHF Data Exchange (VDE-SAT).

These VDES functions are realised through three types of physical components:

1. Mobile stations on ships or other offshore platforms, which integrate AIS, VDES ASM, and VDE functions within one transceiver and operate under the authority of controlling stations.
2. Coastal (shore) controlling stations that manage the operation of mobile stations within their service area; and
3. Satellite (space) stations for global coverage. These can be designed as *receive-only* or *controlling*, with full two-way communication capabilities.

In the following sections, we provide a brief overview of each VDES functional component.

2.2.2. AIS

AIS supports the safety of navigation and maritime domain awareness by conveying a vessel's identity, position, course and other static, dynamic and voyage-related information to other vessels, shore stations and aircraft. It can also be used for transmitting the position and other characteristics of marine Aids to Navigation (AtoN) – both real (or physical, e.g. buoys and lighthouses) and virtual (existing only through an AIS broadcast). Other applications include AIS Search and Rescue Transmitters (AIS SART) and AIS Man Overboard (AIS MOB) devices.

AIS information is packed into a number of message types, each with a specific format and content. The majority of AIS message types have a fixed payload format and are transmitted regularly at pre-defined intervals. For example, AIS Message 1 conveys vessel position reports, whereas AIS Message 21 carries AtoN information.

A small number of AIS message types can be used to send information with a user-defined format and content. Collectively, these are known as AIS Application Specific Messages (AIS ASM).

AIS messages can be addressed to a specific station or broadcast to all stations within range. The transmission interval depends on the message and equipment type and its operational mode and can vary from two seconds to several minutes for the most common message types. For AIS ASM, the transmission interval will typically range from minutes to one-off, on-request transmissions.

AIS messages are transmitted on two radio channels in the upper part of the VHF maritime band, designated as AIS 1 and AIS 2.

The original AIS was designed for terrestrial line-of-sight communication and has a limited range of about 40 nautical miles (depending primarily on the height of the transmitting and receiving antennas). To extend the range of AIS maritime domain awareness services, receivers have been placed on satellites in low Earth orbit; a concept known as Satellite AIS (AIS-SAT). Applications of AIS-SAT include vessel tracking, enhancing search and rescue operations, arrival management and vessel traffic analysis in support of AtoN positioning.

The large number of vessels typically found within the field of view of a satellite can lead to frequent signal collisions, which presents a significant challenge to satellite reception of AIS. To address this problem, an additional two radio channels have been allocated and a new message format defined specifically for satellite reception. This is known as Long Range AIS (LR AIS). The probability of collision is reduced in LR AIS by using a shorter transmission duration and longer update intervals. Vessels transmit the LR AIS messages only when operating outside the range of terrestrial AIS base stations.

2.2.3. VDES ASM

VDES ASM provides dedicated communication channels for the exchange of Application Specific Messages (ASM), alleviating the load on the AIS channels. It builds on the AIS technical specification, with important modifications to the air interface to provide a greater reliability and throughput for ASM transmission.

VDES ASM includes a terrestrial component (VDES ASM-TER) and a satellite component (VDES ASM-SAT). VDES ASM-TER supports addressed and broadcast messages and also offers a 'geographical multicast'/geocast functionality, where messages are sent to all stations within a specified geographic area. The message transmission intervals are expected to be similar to AIS ASM, ranging from minutes to one-off, on-request transmissions.

VDES ASM messages are transmitted on two radio channels in the upper part of the VHF maritime band (designated as ASM 1 and ASM 2). VDES ASM-SAT uses the same two radio channels as VDES ASM-TER, but the radio waveform has been optimised for satellite reception.

2.2.4. VDE-TER

VDE-TER enables two-way data exchange between coastal and mobile stations with a higher throughput than AIS and VDES ASM. A standard set of applications is yet to be defined, but options being considered include cryptographic authentication of AIS and other VDES messages; transport of Maritime Messaging Service (MMS) data within the MCP framework; and ranging mode (R-Mode) as a component of a resilient PNT system of systems.

VDE-TER can be configured to use up to 100 kHz of bandwidth in both the upper and lower parts of the VHF maritime band. Multiple modulation and coding schemes are available to support a wide range of channel conditions and communication requirements. The protocol stack is optimised for the transmission of larger amounts of data than could fit into a single AIS or VDES ASM message, but short messages are also supported.

2.2.5. VDE-SAT

VDE-SAT extends VDE services beyond terrestrial coverage, enabling two-way communication in remote areas, including the high seas and polar regions. Using polar-orbiting satellites, VDE-SAT can achieve global coverage even with a single satellite. However, the communication latency depends on the constellation size, and with small constellations, users will potentially experience delays of up to several hours.

VDE-SAT can be configured to use up to 150 kHz of bandwidth in both parts of the VHF maritime band; however, the spectrum is partly shared with the VDE-TER component. The effective throughput is expected to be lower than for VDE-TER due to regulatory constraints on the downlink signal power and a much larger footprint compared to a terrestrial station.

2.3. SUMMARY OF PERTINENT TECHNICAL CHARACTERISTICS

In assessing the feasibility of different VDES authentication schemes, it is important to consider their impact on the VDES data link load. This section summarises the key technical characteristics of VDES required to make this assessment.

2.3.1. COMMON CHARACTERISTICS

VDES uses a set of radio channels within the maritime mobile VHF band, as defined in the ITU Radio Regulations Appendix 18. These channels can be accessed using various time division multiple access (TDMA) schemes, including fixed access TDMA (FATDMA), self-organised TDMA (SOTDMA) and random access TDMA (RATDMA). The longest unit of time in the VDES TDMA scheme is referred to as a frame. A new frame is established every minute and is uniformly divided into 2250 time slots. VDES transmissions are scheduled in multiples of time slots, with the maximum duration of a transmission depending on the functional component and waveform being used.

VDES stations may use various channel bandwidths, modulation schemes and forward error correction (FEC) rates, depending on the application, functional component and current channel conditions. Consequently, the maximum amount of application data that a single VDES transmission can carry varies significantly based on the component and its specific configuration. The following subsections examine the relationship between the amount of application data queued for transmission and the number of VDES time slots needed to transmit it. The latter will serve as a key metric in assessing the impact of various VDES authentication schemes on the data link load.

2.3.2. AIS

In AIS, user-defined application data is transmitted using Application Specific Messages (AIS ASM). Figure 3 schematically depicts the protocol stack used for AIS ASM transmission, with the overheads introduced at each layer represented by the shaded blocks. As can be seen from the figure, the application data to be transmitted is encapsulated in an AIS message, which is converted into a transmission packet, which then modulates a radio transmitter to produce a transmission that is sent over the air. AIS transmissions occupy between one and five time slots and typically alternate between the two AIS VHF channels to reduce the risk of interference.

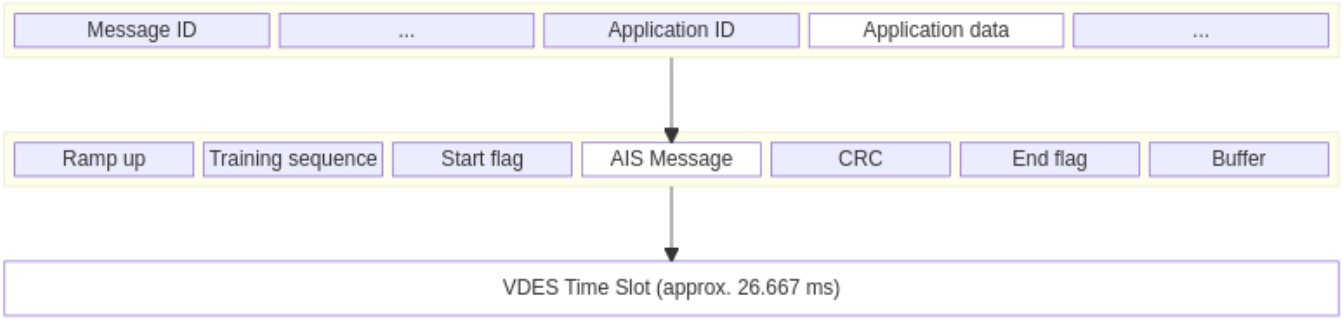

Figure 3 AIS ASM protocol stack

Note: For multi-slot transmissions, only a single application of the overheads shown in Figure 3 is required.

The maximum amount of application data that a single AIS ASM transmission can carry depends on the message type used and the transmission duration. The AIS specification defines four AIS ASM types, and Table 1 shows the maximum application data size (in bits) for each message type as a function of the transmission duration.

Table 1 Maximum application data size (bit) by message type for AIS ASM

AIS Message Type	Message Name	Transmission Duration (slot)				
		1	2	3	4	5
6	Addressed binary message	48	272	496	720	920
8	Broadcast binary message	80	304	528	752	952
25	Single-slot binary message	112	-	-	-	-
26	Multiple-slot binary message with communication state	88	312	536	760	984

Note: AIS transmissions longer than three time slots must be scheduled using FATDMA, which requires coordination with competent national authorities. Such transmissions are also more likely to result in message decoding errors and are discouraged.

The AIS specification further defines 23 single-purpose message types with a fixed payload format. The number of time slots required to transmit each of these message types can be found in Recommendation ITU-R M.1371 [3].

2.3.3. VDES ASM

2.3.3.1. VDES ASM-TER

The overheads introduced by the VDES ASM-TER protocol stack are schematically shown in Figure 4. The application data to be transmitted is encapsulated in a VDES ASM message, which is padded to a fixed length and protected by a cyclic redundancy check (CRC), before being subjected to FEC encoding and bit scrambling. The resulting data is then embedded in a transmission packet, which is modulated onto a radio signal for transmission within one, two or three VDES time slots.

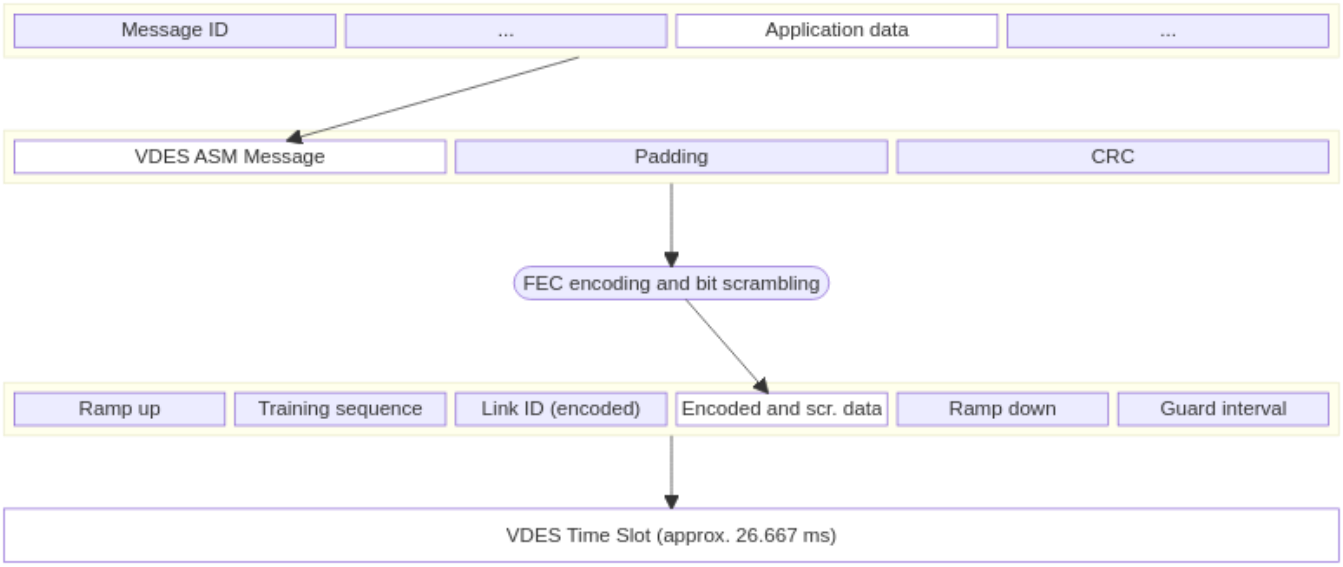

Figure 4 VDES ASM protocol stack

Note: For multi-slot transmissions, only a single application of the overheads shown in Figure 4 is required.

Table 2 provides a summary of the key physical and link-layer characteristics of the VDES ASM-TER air interface. VDES ASM-TER uses transmission durations of up to three time slots, with FEC rates of 1 (no FEC) or 3/4. This results in six possible transmission configurations, known in VDES as *Link IDs*.

Table 2 Selected physical and link-layer characteristics of VDES ASM-TER

Component Characteristic	VDES Link ID					
	1	2	3	5	6	7
Channel Bandwidth (kHz)	25					
Symbol Rate (ksym/sec)	9.6					
Data Modulation	Pi/4-QPSK					
FEC Rate	1 (no FEC)			3/4		
Transmission Duration (slot)	1	2	3	1	2	3
C/N0 Threshold (dB-Hz)	50.8	50.8	50.8	45.1	44.8	44.6

The maximum amount of application data that a single VDES ASM-TER transmission can carry depends on the Link ID and the message type used. The VDES specification defines eight VDES ASM message types, six of which can carry user-defined data, with the remaining two being used for acknowledgement and data link management purposes. Table 3 shows the maximum application data size (in bits) for each VDES ASM message type as a function of the Link ID used.

Table 3 Maximum application data size (bit) by message type for VDES ASM-TER

VDES ASM Message Type	Message Name	VDES Link ID					
		1	2	3	5	6	7
0	Broadcast AIS ASM	296	808	1320	200	584	968
1	Scheduled broadcast message	240	752	1264	144	528	912
2	Broadcast message	280	792	1304	184	568	952
3	Scheduled addressed message	208	720	1232	112	496	880
4	Addressed message	248	760	1272	152	536	920
5	Acknowledgement message	-	-	-	-	-	-
6	Geographical multicast message	208	720	1232	112	496	880
7	ASM data link management message	-	-	-	-	-	-

Note: For VDES ASM message type 0, Broadcast AIS ASM, the application data encapsulates an entire AIS message 6, 8, 12, 14, 21, 25 or 26. Consequently, the application data size actually available also depends on the AIS message type being encapsulated.

For the transmission of larger amounts of data than can fit into a single VDES ASM-TER message, the VDES specification defines the Multiple Incremental TDMA (MITDMA) channel access scheme. MITDMA allows a VDES station to chain up to 15 transmissions together in a single frame, each up to three time slots long. MITDMA is used with VDES ASM message types 1, 3 and 5.

The number of time slots required to transmit a given amount of application data over VDES ASM-TER can be determined using the following procedure:

1. Determine the appropriate VDES ASM message type for the application data to be transmitted.
2. Choose the appropriate VDES Link ID based on the required reliability and application data size.
3. Calculate the number of messages required to transmit the application data, based on the maximum application data size for the chosen message type and Link ID.
4. Calculate the total number of time slots required to transmit the messages, based on the transmission duration of the chosen Link ID and the number of messages.

2.3.3.2. VDES ASM-SAT

The VDES ASM-SAT protocol stack introduces overheads in a similar manner to VDES ASM-TER (see Figure 4), with the key difference being the use of a longer guard interval to account for the increased propagation delays associated with satellite communications. As a result, the maximum application data sizes are slightly reduced compared to VDES ASM-TER.

The key characteristics of the VDES ASM-SAT air interface are summarised in Table 4. There is only one Link ID defined for the VDES ASM-SAT uplink, which uses a transmission duration of three time slots and a FEC rate of 3/4.

Table 4 Selected physical and link-layer characteristics of VDES ASM-SAT

Component Characteristic	VDES Link ID
	4
Channel Bandwidth (kHz)	25
Symbol Rate (ksym/sec)	9.6
Data Modulation	Pi/4-QPSK
FEC Rate	3/4
Transmission Duration (slot)	3
C/N0 Threshold (dB-Hz)	44.3

The maximum application data size (in bits) for each VDES ASM message type when transmitted using the VDES ASM-SAT Link ID is shown in Table 5.

Table 5 Maximum application data size (bit) by message type for VDES ASM-SAT

VDES ASM Message Type	Message Name	VDES Link ID
		4
0	Broadcast AIS ASM (terrestrial use only)	-
1	Scheduled broadcast message	808
2	Broadcast message	848
3	Scheduled addressed message	776
4	Addressed message	816
5	Acknowledgement message	-
6	Geographical multicast message	776

As in VDES ASM-TER, up to 15 VDES ASM-SAT messages can be chained together in a single frame using the MITDMA channel access scheme.

The number of time slots required to transmit a given amount of application data over VDES ASM-SAT can be determined by following the same procedure as for VDES ASM-TER, noting the different Link ID used for VDES ASM-SAT.

2.3.4. VDE-TER

IALA recommends that each logical unit of application data sent over VDE be accompanied by a 16-bit VDE Protocol Format Identifier (VPFI) and, optionally, an 8-bit to 16-bit VDE Protocol Format Message Identifier (VPFMI) [1]. This data is then encapsulated in variable-length segments, each of which corresponds to an individual transaction at the VDES transceiver's presentation interface. Each segment introduces an additional 32 bits of overhead.

Segments are transported in VDE-TER messages. A segment may span multiple VDE-TER fragment messages, as illustrated in Figure 5; however, it is also possible to encapsulate multiple segments in a single VDE-TER message, as shown in Figure 6.

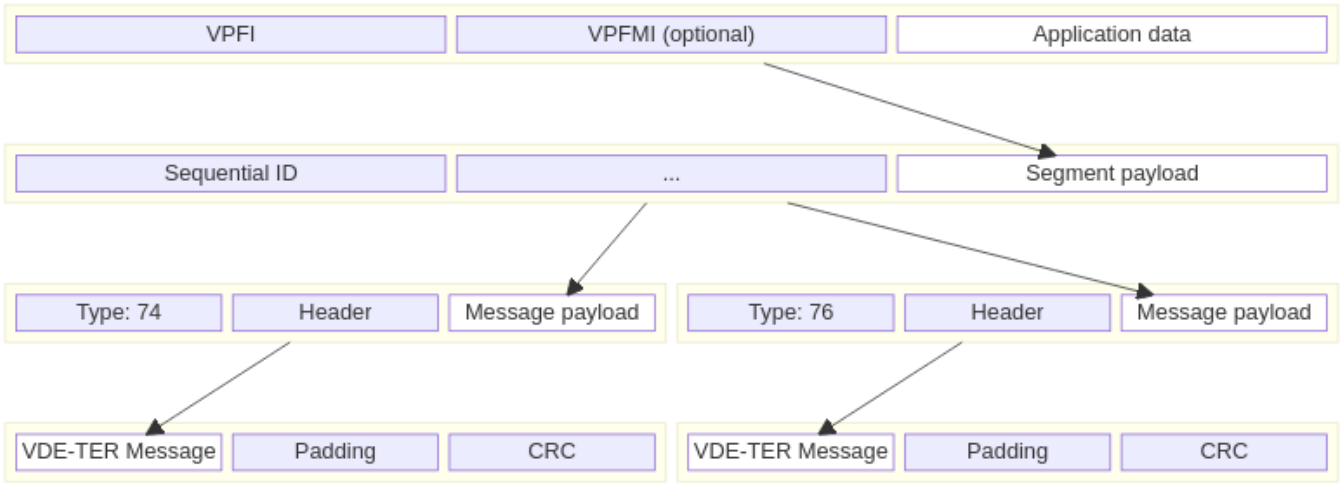

Figure 5 VDE-TER protocol stack – segment spanning multiple fragments

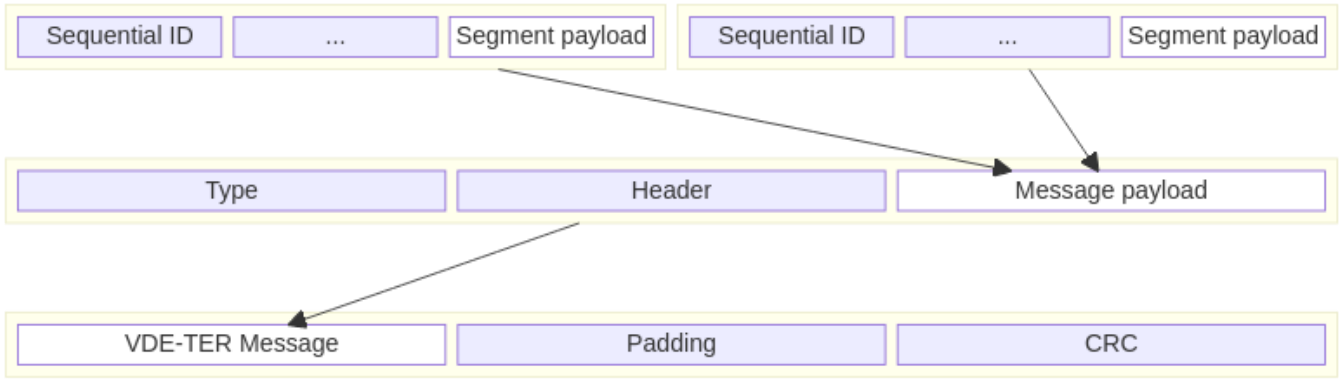

Figure 6 VDE-TER protocol stack – multiple segments in a single message

A VDE-TER message consists of a Type field, a header and a message payload that carries one or more segments. The header includes a Length field and a Source ID field that identifies the data source. The Source ID ranges from 0 to $2^{32} - 1$. Values from 0 to 999999999 represent a maritime mobile service identity (MMSI), as defined in Recommendation ITU-R M.585 and assigned to a VDES station by the relevant national administration. Values outside this range are reserved for future use.

The VDE-TER messages are padded to a fixed length and protected by a CRC, as also shown in Figure 5 and Figure 6, before being subjected to FEC encoding and bit scrambling, in a similar manner to VDES ASM-TER (see Figure 4).

Note: The padded and CRC-protected VDE-TER message is also known as a VDE packet in the VDES specification. A VDE packet may encapsulate multiple VDE-TER messages.

The resulting data is then embedded in a transmission packet, which is modulated onto a radio signal for transmission. A VDE transmission packet is always sent over the air in a single time slot.

The VDES specification defines thirteen Link IDs for terrestrial VDE use; however, six of those are currently marked as optional and another four are reserved for radionavigation purposes (R-Mode). Table 6 summarises the key physical and link-layer characteristics of the three remaining VDE-TER Link IDs.

Table 6 Selected physical and link-layer characteristics of VDE-TER

Component Characteristic	VDES Link ID		
	11	17	19
Channel Bandwidth (kHz)	25	100	
Symbol Rate (ksym/sec)	19.2	76.8	
Data Modulation	Pi/4-QPSK		16-QAM
FEC Rate	1/2		3/4
Transmission Duration (slot)	1		
C/N0 Threshold (dB-Hz)	43.8	49.9	59.1

The VDES specification defines thirteen VDE-TER message types. Eight of these are used for signalling purposes, while the remaining five can carry user-defined data:

- Message types 92 and 93 are used for short data message transmissions within one time slot.
- Message types 74, 75 and 76 can be used to transmit arbitrarily large amounts of data by linking multiple messages together in a data session.

Table 7 shows the maximum message payload size (in bits) for the five mentioned VDE-TER message types, as a function of the Link ID used. Note that additional overheads are introduced due to segmentation and the VPFI/VPFMI fields. Consequently, the amount of application data that can be transmitted in a single VDE-TER message depends on the number of segments and the size of the VPFMI field(s) used and will be lower than the maximum message payload size shown in table.

Table 7 Maximum message payload size (bit) by message type for VDE-TER

VDE Message Type	Message Name	VDES Link ID		
		11	17	19
74	Start fragment	280	1720	5464
75	Continuation fragment	280	1720	5464
76	End fragment	280	1720	5464
92	Short data message (with ACK)	296	1736	5480
93	Short data message (no ACK)	304	1744	5488

The VDES specification defines ten VDE-TER data transfer protocols, each of which is associated with a specific set of VDE-TER message types. For details of these protocols, consult Recommendation ITU-R M.2092 [4]. Suffice it to say that there are two classes of VDE-TER protocols:

- short data message protocols, using message types 92 and 93; and
- data session protocols, using message types 74, 75 and 76 among others.

A VDES unit selects the appropriate protocol based primarily on the amount of data to be transmitted. If the data queued for transmission can be sent within ten time slots, and each individual data segment fits in one short data message (types 92 or 93), a short data message protocol is used. Otherwise, a resource allocation must be made for a data session transfer, in which case a minimum of 45 slots are allocated to the transmitting station, and an additional slot is used for the resource allocation. If messages that exceed the payload space of a short data message are sent very frequently, 375 slots – corresponding to one TDMA channel (a concept which will not be discussed in detail here) - would be permanently allocated to this use. It is noted that if the transmitting station has no other data to send, the remaining slots cannot be used by another station and thus will go unused.

The number of time slots required to transmit a given amount of application data over VDE-TER can be determined using the following procedure:

1. Determine the appropriate VPFI and, if applicable, VPFMI for the application data to be transmitted. Consult IALA Guideline 1117 for examples of VPFI and VPFMI assignments and the corresponding application data formats [cite:iala-g1117].
2. Calculate the size of the resulting VDE segment (or segments, if multiple presentation interface transactions are required).
3. Determine whether a short data message protocol or a data session protocol is required based on the number and size of the segments.
4. Calculate the number of VDE-TER messages required to transmit the segment(s). Assuming that each message is converted into a single VDE/transmission packet, the number of VDE-TER messages is equal to the number of time slots used. If using a data session protocol, note also the number of time slots allocated for the transmission, in addition to the slots actually used.

2.3.5. VDE-SAT

The VDE-SAT protocol stack introduces overheads in a similar manner to VDE-TER, with the key difference being the use of a longer guard interval to account for the increased propagation delays associated with satellite communications. VDE-SAT also uses pilot symbols and, in some cases, longer or additional training sequences (also known as 'syncwords') to aid in channel estimation.

The VDES specification defines five Link IDs for satellite VDE uplink, with one of those currently marked as optional. Table 8 summarises the key characteristics of the four recommended VDE-SAT Link IDs.

Table 8 Selected physical and link-layer characteristics for VDE-SAT uplink

Component Characteristic	VDES Link ID			
	20	21	22	24
Channel Bandwidth (kHz)	50			
Symbol Rate (ksym/sec)	2.1	33.6		
Data Modulation	QPSK/CDMA	Pi/4-QPSK		16-QAM
FEC Rate	1/4	2/3		5/6
Transmission Duration (slot)	5	1	3	
C/N0 Threshold (dB-Hz)	32.3	49.2	49.2	57.5

The VDES specification defines 28 VDE-SAT message types. Ten of these can carry user-defined data in the mobile-to-satellite direction (uplink):

- Message types 23 to 28 and 33 are used for short data message transmissions in five time slots.
- Message types 30, 31 and 32 can be used to transmit larger amounts of data by linking multiple messages together in a data session.

Table 9 shows the maximum payload size (in bits) for the ten mentioned VDE-SAT message types, as a function of the Link ID used.

Table 9 Maximum message payload size (bit) by message type for VDE-SAT uplink

VDE Message Type	Message Name	VDES Link ID			
		20	21	22	24
23	Uplink short data message (without ACK)	8	-	-	-
24-28	Uplink short data message (without ACK, without Destination ID)	40	-	-	-
30	Start fragment	-	584	2968	7424
31	Continuation fragment	-	584	2968	7424
32	End fragment	-	584	2968	7424
33	Uplink short data message (with ACK)	8	-	-	-

Note: Short data messages are always transmitted using VDES Link ID 20.

Note: The start, continuation and end fragment message overheads exceed the maximum message size for VDES Link ID 20.

The VDES specification defines eight Link IDs for use in satellite VDE downlink. Their key characteristics are summarised in Table 10.

Table 10 Selected physical and link-layer characteristics for VDE-SAT downlink

Component Characteristic	VDES Link ID							
	25	26	27	28	29	32	33	34
Channel Bandwidth (kHz)	50			100	150	50		
Symbol Rate (ksym/sec)	4.2	33.6		36	56.4	4.2	33.6	
Data Modulation	BPSK/CDMA	Pi/4-QPSK	8-PSK	BPSK/CDMA			BPSK	Pi/4-QPSK
FEC Rate	1/2	1/4	1/2	1/4			1/3	
Transmission Duration (slot)	90					15		
C/N0 Threshold (dB-Hz)	34.2	42.9	50.3	40.6	42.5	31.6	41.7	44.7

There are 28 VDE-SAT message types, five of which can carry user-defined data in the satellite-to-mobile direction (downlink):

- Message types 14 and 16 are used for short data message transmissions in 90 or 15 time slots (depending on the Link ID used).
- Message types 30, 31 and 32 can be used to transmit larger amounts of data by linking multiple messages together in a data session.

Table 11 shows the maximum payload size (in bits) for the five mentioned VDE-SAT message types, as a function of the Link ID used.

Table 11 Maximum message payload size (bit) by message type for VDE-SAT downlink

VDE Message Type	Message Name	VDES Link ID							
		25	26	27	28	29	32	33	34
14	Downlink short data message (with ACK)	4648	38064	114480	20992	33184	184	4152	8192
16	Downlink short data message (without ACK)	4648	38064	114480	20992	33184	184	4152	8192
30	Start fragment	4624	38040	114456	20968	33160	160	4128	8168
31	Continuation fragment	4624	38040	114456	20968	33160	160	4128	8168
32	End fragment	4624	38040	114456	20968	33160	160	4128	8168

The VDES specification defines eight VDE-SAT data transfer protocols, each of which is associated with a specific set of VDE-SAT message types. For details of these protocols, consult Recommendation ITU-R M.2092 [4]. As with VDE-TER, short data message protocols can be used to transmit small amounts of data with minimal overhead, while data session protocols are used for larger data transfers and require a resource allocation.

The number of time slots required to transmit a given amount of application data over VDE-SAT can be determined using essentially the same procedure used for VDE-TER, with main difference being the use of different message types and Link IDs.

3. FUNDAMENTAL CONCEPTS OF CRYPTOGRAPHIC AUTHENTICATION

3.1. DISTINCTION BETWEEN AUTHENTICATION AND ENCRYPTION

Encryption refers to the process of 'scrambling' data to prevent unauthorised users from reading sensitive data, thereby ensuring privacy.

Authentication refers to verifying data is from a legitimate source. This is typically accomplished by signing the data using a digital signature. A digital signature can prove both data origin (i.e. that it is from a legitimate source and not spoofed by an unauthorised third party) and integrity (i.e. that data has not been accidentally or maliciously changed in transit).

Authentication of data, and particularly data ascertaining to the safe navigation of a vessel, is necessary to prevent spoofing. The need to authenticate maritime data is growing, given the increasing ease with which maritime data communications may be spoofed, and the increasing availability and dependence on such data.

The need to routinely authenticate data is recognised by IALA; IALA Recommendation R1024 *Cyber security for the IALA domain* states that 'IALA members work towards the goal of ensuring all data in the IALA domain is provided with a means to authenticate the data'.

3.2. SYMMETRIC VS. ASYMMETRIC CRYPTOGRAPHY AND DIGITAL SIGNATURES

Symmetric encryption and symmetric authentication make use of a secret key (akin to a single 'secret password') to encrypt and decrypt data and/or "digitally sign" and verify data. A copy of the secret key must be issued to all users for them to secure the data sent to each other. All copies of the secret, shared key must be kept very secure as access to this key will allow both eavesdropping (decryption) of communications by a third party and will also allow a third party to digitally "sign" false or malicious communications.

A serious drawback of symmetric encryption is the need to share and distribute the secret key securely; before any two groups can exchange encrypted or signed data, they first need to meet securely in order to agree on and share

a secret key between themselves. For many maritime applications, this is highly impractical; it is not possible for every vessel to previously meet with, and securely exchange a secret key with, every other vessel, port, vessel traffic service and other entity with whom they may wish to communicate.

Asymmetric encryption and asymmetric authentication makes use of two mathematically linked keys; a public key which is published and widely disseminated (often published prominently on the internet), and a private key which is kept secret and known only to an individual user. This circumvents the need for a secure meeting to exchange a symmetric, secret key. Note that assymetric cryptography is also known as public key cryptography (PKC).

For encryption, the sender uses the openly available public key to encrypt messages (this avoids the need to securely meet and agree on a secret shared key beforehand). Once encrypted, only the intended recipient is able to decrypt the data using their private key.

To sign data messages, the following procedure is commonly used:

- The sender first uses a hashing algorithm on the data to be signed. This algorithm maps data of an arbitrary size to a separate, short, fixed-size string of characters. This separate string of characters is known as a digest.
- The sender uses their own private key to encrypt a copy of the digest, thus forming a digital signature. This digital signature is sent to the recipient alongside the data message.
- To determine if the data message is genuine, the recipient may use the openly available public key to decrypt the signature and use the hashing algorithm on the data message to create their own copy of the message digest. If the decrypted signature and message digest match, then the signature can only have been made using the sender's private key, thereby indicating the data message is genuine

Numerous symmetric and asymmetric cryptographic algorithms are available providing varying levels of security, encryption/decryption speed and signature size. As the quality of these algorithms can vary, it is recommended that when choosing any encryption algorithm only algorithms subjected to extensive cryptanalysis and therefore considered secure are used; further noting that maritime communications may be subjected to, and need to resist, dedicated professional cyber-attack.

3.3. TESLA (TIMED EFFICIENT STREAM LOSS-TOLERANT AUTHENTICATION)

A disadvantage of digital signatures is that their introduction and use will inevitably increase channel loading. This may be particularly problematic at VHF frequencies where data rates are relatively low, and when using crowded AIS channels.

One approach to minimise channel loading is to use signatures pertaining to the previous n data messages rather than signing each and every data message. Normally, using this approach will be problematic, as should one data message be missed or fail to be received, the user will then be unable to authenticate all n data messages.

The TESLA protocol, however, makes it possible for a single digital signature to effectively sign multiple data messages in a manner that allows the remaining data messages to be safely authenticated even if some of them are missing. This is accomplished through a combination of symmetric and asymmetric cryptographic techniques. A detailed description of TESLA is beyond the scope of this document; therefore, the reader is referred to the following reference for further information [5].

Given the above, the TESLA protocol may be a practical option for limiting data channel loading due to the introduction of digital signatures. However, using the TESLA protocol is likely to increase the complexity of an authentication solution. Its use is therefore likely to be inappropriate where low channel loading does not justify its introduction. Similarly, TESLA is unlikely to provide useful benefits when messages are sent infrequently, such as in the case of a single Virtual AIS AtoN or a Meteorological and Hydrological Data broadcast.

3.4. PUBLIC KEY INFRASTRUCTURE

Asymmetric cryptography enormously simplifies 'key management' as public keys may simply be published openly without the need to exchange them securely. However, there are a number of outstanding issues relating to key management detailed as follows:

- A user needs to be sure the public key they have obtained has (i) not been tampered with, and (ii) really does belong to the entity that the public key says it belongs to and not an imposter (i.e. each public key must be verifiably associated with the correct identity).
- Public keys must be easy to obtain and distribute. Every vessel and shore station must be able to immediately access every public key it is likely to need, including recently created public keys.
- Large numbers of public keys from numerous vessels, VTS, coastguard and other authorities may cause the number of keys in circulation (the public key almanac) to become large and unwieldy.
- A mechanism needs to be in place so that, should a private key be stolen, compromised or lost, the corresponding public key can be revoked.

These matters must be addressed through the development of an appropriate *public key infrastructure (PKI)*; a system for managing public keys that meets the specific needs of the mariner.

The Maritime Identity Registry (MIR), a component of the MCP is IALAs preferred approach to establishing a PKI. Information on the MIR and its use may be found in IALA Guideline G1183 *The Provision of Maritime Connectivity Platform (MCP) Identities*. It is noted that the MIR is compatible with the IEC 63173-2 'SECOM' standard for secure transfer of S-100 data using Internet Protocol (IP)-based communications.

3.5. CERTIFICATE AUTHORITIES

A certificate authority (CA) is a third party which is well known, respected, and universally trusted by all users. The CA's main function is to verify the authenticity of public keys. It does so by conducting in-depth checks as to the ownership of public keys. Once the CA is satisfied that the public key belongs to the entity it reports to belong to, the CA will digitally sign the public key, creating an attached security certificate. Any user would see the CAs security certificate (the CAs trusted digital signature) on a public key and will know that the public key is genuine, assuming they have trust in the CA.

Furthermore, should the public key be tampered with, the public key will be different from that digitally signed by the CA and the user will be alerted as to a 'failed' CA signature.

Any organisation, such as a shipping company, lighthouse authority or international organisation (such as IALA or the IMO) may act as a CA. It is the decision of end users to choose which CAs they wish to trust.

The MIR has developed processes to simplify the delegation of CA trust. These are described in IALA Guideline G1183.

It may also be worth noting that the IMO currently acts as a PKI Certificate Authority for the Long-range Identification and Tracking (LRIT) system. For details, refer to IMO MSC.1/Circ.1376/Rev.5.

3.6. AUTHENTICATION VS. TRUST

Cryptographic authentication ensures that the communication between a source and a user is secure and that the message truly comes from the claimed source. However, authentication does not guarantee the truthfulness or validity of the content. A source can still transmit false or misleading information, whether intentionally or due to errors (e.g. malfunctioning sensors).

Trust – the confidence in the truth or reliability of the information - comes from other factors such as reputation.

4. UNDERSTANDING THE POTENTIAL CYBER SECURITY RISKS TO VDES

4.1. PHYSICAL TAMPERING

Physical tampering with VDES and GNSS equipment, such as accessing internal interfaces by opening a device, can potentially allow unauthorized access, data injection, or disruption of VDES operations. This document assumes that appropriate physical security measures are implemented to protect equipment and associated infrastructure from tampering; therefore, this attack vector is not addressed further.

4.2. GNSS DENIAL (JAMMING / INFRASTRUCTURE ATTACKS)

GNSS service denial can be caused by:

- Jamming, where an attacker transmits interfering signals in the GNSS frequency band(s) to overpower legitimate transmissions; or
- Cyber or physical attacks against GNSS ground infrastructure or satellites, causing service disruptions.

VDES typically relies on GNSS for transceiver synchronization and positioning. A GNSS outage can therefore:

- Disrupt accurate transmission timing within the VDES TDMA frame structure, leading to transmission collisions and reduced throughput; and
- Prevent accurate position reporting by VDES transceivers, which may impact the ability of nearby vessels and shore-based systems to track and communicate with the affected vessels.

The AIS specification includes several fallback mechanisms that allow transceivers to synchronize their transmissions to other AIS stations in the absence of GNSS timing, thereby maintaining a basic level of service. For other VDES components, fallback timing support is partially addressed through the inclusion of 'UTC Indirect' in both VDES ASM and VDE. Other mechanisms, such as 'semaphore mode' known from AIS, have not been defined for these VDES components.

Potential mitigation measures include failsafe system and service design, hardening of GNSS receivers against jamming and the use of multiple Position, Navigation and Timing (PNT) sources, as described in IALA Guideline G1180 *Resilient Position, Navigation and Timing*.

4.3. GNSS SPOOFING AND MEACONING

GNSS spoofing involves the transmission of false GNSS signals to deceive GNSS receivers into reporting incorrect information.

GNSS meaconing refers to the recording and replaying of legitimate GNSS signals at a later time to deceive GNSS receivers.

GNSS spoofing and meaconing can impact VDES operations in several ways:

- Timing disruption: VDES transceivers may accept spoofed GNSS signals as legitimate, erroneously shifting their internal clocks. This can lead to misalignment of the TDMA frame structure, causing transmission collisions and reduced throughput.
- Data link disruption: Spoofing/meaconing leads a VDES station to believe it is in a different location than it actually is. This makes service area-based access control unreliable and can lead to incorrect protocol or frequency channel usage.

- Incorrect position, velocity and time reporting: VDES transceivers affected by GNSS spoofing/meaconing may report incorrect positions, velocities and times, with potentially severe consequences for maritime safety.
- Undermined cryptographic protections (time-based): Spoofing/meaconing can also undermine cryptographic protections that rely on accurate time synchronisation, such as the inclusion of cryptographically protected timestamps in VDES messages.

The effects of GNSS spoofing and meaconing can be mitigated through the use of multiple PNT sources, ideally secured by cryptographic means, as described in IALA Guideline G1180 *Resilient Position, Navigation and Timing*.

VDES authentication may play a role in detecting GNSS spoofing/meaconing attacks and alerting users to the presence of potentially malicious data

4.4. VDES JAMMING

VDES jamming involves the transmission of interfering signals in the VDES frequency band(s) to prevent legitimate VDES transmissions from being received. The consequence is a denial or degradation of service for VDES users in the affected area.

Potential mitigation measures include spectrum and VDES data link performance monitoring and follow-up actions, as described in IALA Guideline G1181 *VDES VHF Data Link (VDL) Integrity Monitoring*

4.5. VDES SPOOFING

VDES spoofing involves transmitting signals that emulate legitimate VDES transmissions, with the goal of deceiving VDES receivers or their users into accepting malicious information. Spoofing can target different layers of the VDES protocol stack, as outlined below.

4.5.1. SPOOFING SIGNALLING MESSAGES

VDES signalling messages include the VDES ASM Data link management message, VDE-TER Media access control, Resource allocation, Bulletin board and other messages that control channel access and data transmission on the VDES data link. Sending counterfeit signalling messages that allocate resources or change channel access parameters could lead to service disruption or denial for legitimate VDES users.

Cryptographic authentication may be employed to safeguard VDES signalling messages against spoofing. By enabling the detection of potentially malicious transmissions, a VDES transceiver can either reject such messages outright or alert the user to their presence.

It is anticipated that the mechanism for the authentication of VDES signalling messages will be defined in ITU-R Recommendation M.2092 *Technical characteristics for a VHF data exchange system in the VHF maritime mobile band* and the applicable IEC equipment standards. Therefore, this document does not provide detailed guidance on this topic. Currently, Rec. ITU-R M.2092 includes provisions for the authentication of Bulletin board messages. Authentication of other signalling messages can be achieved by other means.

4.5.2. SPOOFING APPLICATION DATA MESSAGES

VDES may be used in a wide range of maritime applications, including conveying navigation-related messages. Therefore, spoofing VDES messages that carry application data, such as AIS position reports, Application Specific Messages and VDE-TER or VDE-SAT fragments can have serious consequences for maritime safety, including directing ships into harm. Flooding VDES transceivers and associated systems with large volumes of spurious application data can also lead to service denial or degradation.

Due to the critical nature of this threat, securing VDES application data through cryptographic authentication should be top priority and is the primary focus of this document. To achieve this, proven cryptographic techniques can be

applied, such as digital signatures or the TESLA protocol. Application data that fails authentication should be flagged to the user or rejected.

4.5.3. SPOOFING R-MODE SIGNALS

Falsifying VDES R-Mode transmissions can lead to incorrect position and timing information being presented to VDES users if R-Mode is used as a PNT source.

For R-Mode to be considered a credible backup to, or integrity checking mechanism for, GNSS, it is essential that R-Mode signals provide at least the same level of cyber security as GNSS signals. Given that at least one of the established GNSS constellations now allows for a cryptographic authentication of its navigation messages, we recommend that R-Mode signals be similarly protected.

Radionavigation signals, such as R-Mode, typically have two components – the navigation message, which carries information such as transmitter location and other system parameters, and the ranging signal, which is used to determine the (pseudo)distances between the transmitters and the receiver. Ideally, both components should be protected against spoofing.

The R-Mode navigation messages are sent at a much lower rate than the ranging signals (typically once a minute) and could be protected using the same techniques as other VDES application data messages.

The ranging signals are normally known, fixed waveforms that may be sent at short (e.g. one or two-second) intervals. This necessitates a different approach to authentication. A potential solution that involves varying the ranging sequences in an unpredictable manner with a subsequent verification using a TESLA-secured navigation message is described in references [6] and [7].

For further information on VDES R-Mode, refer to IALA Guideline G1158 VDES R-Mode. A detailed vulnerability analysis of VDES R-Mode can be found in [8].

It is anticipated that the preferred authentication mechanism for R-Mode signals will be defined in a future edition of this document.

4.6. VDES MEACONING

VDES meaconing refers to the recording and replaying of legitimate VDES signals at a later time to deceive VDES receivers or their users. Similar to spoofing, meaconing can target different layers of the VDES protocol stack, as discussed below.

4.6.1. MEACONING SIGNALLING AND APPLICATION DATA MESSAGES

Meaconing VDES signalling messages can lead to service disruption or denial for legitimate VDES users, while replaying VDES application data messages has the potential to mislead VDES users and compromise maritime safety.

This type of attack can be rendered ineffective by including cryptographically protected sequence or version numbers and time stamps in VDES messages, such that replayed messages can be detected and rejected. Note, however, that the successful use of time stamps for this purpose requires that the recipient has access to a trusted source of time, which may require additional security measures (as discussed in the section on GNSS spoofing and meaconing).

4.6.2. MEACONING R-MODE SIGNALS

As with spoofing, the meaconing of VDES R-Mode signals can result in erroneous position and timing information being presented to users, potentially compromising maritime safety.

Cryptographic methods can provide only partial protection against such attacks. While the authentication of navigation messages and validation of their time stamps can ensure that replayed data is recognised as outdated once its validity period expires, these measures do not extend to the ranging signals. Although cryptographic techniques can confirm that a ranging sequence originated from a legitimate source, they cannot prevent an

adversary from replaying that signal within the valid timeframe. It should be noted that while R-Mode navigation data typically has a validity period of approximately one minute, a ranging signal replayed with a delay of only a few hundred nanoseconds can still introduce significant positioning errors.

To effectively mitigate this threat, a combined approach is recommended. Cryptographic authentication of navigation messages should be complemented by non-cryptographic techniques, such as detection of inconsistencies in signal direction of arrival, receiver motion or timing, to detect and flag potentially malicious replay.

4.7. NETWORK AND SYSTEM INTEGRATION THREATS

As VDES becomes integrated with other shipboard and shore-side systems and networks, it may inherit vulnerabilities at the network interface level. These vulnerabilities could be exploited by attackers to compromise the integrity or functionality of VDES applications.

To mitigate such risks, system integrators should adhere to established industry standards for network security and apply best practices for secure system design and integration. Implementing cryptographic authentication at the application level (providing true end-to-end security) can mitigate the effects of network-level attacks, ensuring that data remains trustworthy even if underlying networks are compromised.

4.8. SUMMARY

The table below provides and overview of identified attack vectors relevant to the VDES environment, along with an assessment of whether cryptographic authentication can mitigate each threat. The mitigation potential is indicated using one of three descriptors:

- **Yes**: Cryptographic authentication can directly mitigate or neutralise the attack.
- **No**: Cryptographic authentication has no impact; alternative measures are required.
- **Partially**: Authentication can aid in detection or containment (e.g. by identifying replayed data), but cannot fully prevent the attack.

Table 12 Identified attack vectors relevant to the VDES environment

Attack Vector	Brief Description	Mitigated by VDES Authentication?
Physical Tampering	Gaining unauthorized physical access to equipment internals or interfaces	No
GNSS Denial	Jamming or cyber/physical attacks against GNSS infrastructure	No
GNSS Spoofing & Meaconing	Transmission of false or previously recorded GNSS signals	No
VDES Jamming	Overpowering legitimate VDES transmissions	No
VDES Spoofing	Transmission of false VDES signals	Yes
VDES Meaconing	Replay of legitimate VDES signals	Partially
Network / Integration Threats	Exploiting vulnerabilities in network interfaces	Partially

5. CHALLENGES TO VDES AUTHENTICATION

This section outlines the principal challenges to implementing an authentication scheme for VDES. For a more detailed treatment, readers are refered to reference [9].

5.1. BACKWARD COMPATIBILITY REQUIREMENTS

The AIS is mandated under the Safety of Life at Sea (SOLAS) Convention and is therefore widely deployed across the global maritime fleet. As such, any new AIS authentication scheme must preserve full compatibility with these existing systems, working within the confines of the existing AIS protocol and the mariners' established practices. This constraint significantly limits the design space for AIS authentication schemes.

Legacy devices must be able to receive and interpret data without restriction, regardless of whether those messages are authenticated. Consequently, authentication mechanisms must be deployed in a manner that does not require changes to existing AIS message formats or transmission behaviours.

In contrast, other components of VDES – VDES ASM, VDE-TER and VDE-SAT, are not yet broadly deployed, which provides more flexibility in the design of authentication schemes for these components.

5.2. CAPACITY LIMITATIONS

VDES communication links operate at significantly lower data rates than terrestrial or satellite broadband systems. Cryptographic authentication, particularly when based on PKC, involves the exchange of relatively large amounts of data such as public key certificates and digital signatures. The constrained capacity of VDES links presents significant challenges to accommodating such data overheads. Any authentication scheme must therefore be carefully designed to minimise resource consumption while still ensuring robust security.

5.3. CHALLENGES OF A MARITIME PKI

The establishment of a global maritime PKI, such as would be required for VDES authentication, presents a number of challenges.

Maritime vessels often operate with intermittent connectivity to shore infrastructure, complicating the timely update of public key certificates and distribution of certificate revocation lists. Moreover, a maritime PKI must scale to accommodate a wide array of actors – including vessels, AtoN, vessel traffic services and other entities - across jurisdictions with varied governance structures.

To address these challenges, maritime-specific certificate authorities (CAs) may be established under the auspices of recognised maritime organisations. These CAs would be directly accountable to maritime stakeholders and more accommodating to their unique needs than generic CAs. An example of such an approach, relying on the use of MCP MIR, may be found in IALA Guideline G1183 *Provision of MCP Identities*.

5.4. QUANTUM COMPUTING AND LONG-TERM IMPLICATIONS

Quantum computers are a new type of computing device that use the properties of quantum mechanics to perform calculations. They have the potential to solve certain mathematical problems underpinning many PKC algorithms much faster than classical computers, potentially allowing attackers to forge digital signatures.

Recognising this risk, many national cybersecurity authorities now advocate for a transition to quantum-safe cryptography (QSC) [11].

Maritime technologies tend to have slow approval processes and, once in service, are expected to remain in use for decades. Given these long timescales, it is suggested that a VDES authentication scheme may need to provide a means to transition to new cryptographic algorithms as they become available.

It must also be noted that quantum-safe digital signatures tend to be significantly larger than their classical counterparts - often by a factor of 10 for equivalent security levels - exacerbating the existing capacity limitations of VDES data links.

5.5. EXPORT RESTRICTIONS ON CRYPTOGRAPHIC TECHNOLOGIES

When designing VDES authentication schemes, it is essential to consider international export controls that apply to cryptographic technologies.

Although cryptographic authentication mechanisms (such as digital signatures) are generally not subject to export restrictions, cryptographic encryption schemes frequently are. Restrictions depend on factors such as algorithm strength, intended use, destination country and applicable domestic legislation.

As this guideline cannot provide legal advice, it is the responsibility of exporters to verify and comply with relevant national and international export control regimes.

6. AUTHENTICATION REQUIREMENTS

6.1. USE CASES

This section identifies high-priority e-navigation use cases that form the basis for defining the requirements of the VDES authentication schemes proposed in this guideline. Each use case is described in terms of the VDES components involved, the message type(s) used, the Link ID(s) used, the number of time slots per transmission, the transmission interval and the proposed maximum allowable authentication delay (time to authentication).

In this first edition of the guideline, the scope of considered use cases is limited to the Virtual AIS AtoN.

6.1.1. VIRTUAL AIS ATON

6.1.1.1. Overview

A Virtual AIS AtoN represents an AtoN that exists only as a digital symbol and is broadcast via AIS without the presence of a physical structure at the reported location. These Virtual AtoN appear on AIS-capable shipborne displays (e.g. ECDIS, radar) just like physical buoys or beacons, but are entirely software-generated.

They are typically used to mark new or temporary hazards, define temporary routes or restricted areas, or provide navigational marking in areas where installing a physical AtoN is impractical or unsafe.

6.1.1.2. VDES Components & Message Type(s)

Virtual AIS AtoN are most commonly implemented using AIS message type 21 (Aid to Navigation Report), with the 'Virtual' flag set.

In addition to point-based Virtual AIS AtoN, AIS ASM, such as the Area Notice, may also be used to define zones, routes or polygon-based navigation features [12].

6.1.1.3. Time Slots per Transmission

AIS message type 21 is transmitted using two time slots.

6.1.1.4. Transmission Interval

According to IMO, ITU and IALA recommendations, the nominal transmission interval for message type 21 is three minutes (180 seconds). If no update is received within 15 minutes, the Virtual AIS AtoN should be considered lost and removed from the display.

6.1.1.5. Authentication Delay

The authentication delay – also referred to as time to authentication – is the maximum permissible time between reception of a message and its successful authentication by the receiving system.

While a shorter authentication delay is generally preferable, accepting a longer time to authentication can reduce the associated data and processing overheads.

A practical upper limit of one minute (60 seconds) is proposed, which ensures that anomalies can be flagged well in advance of the next scheduled transmission.

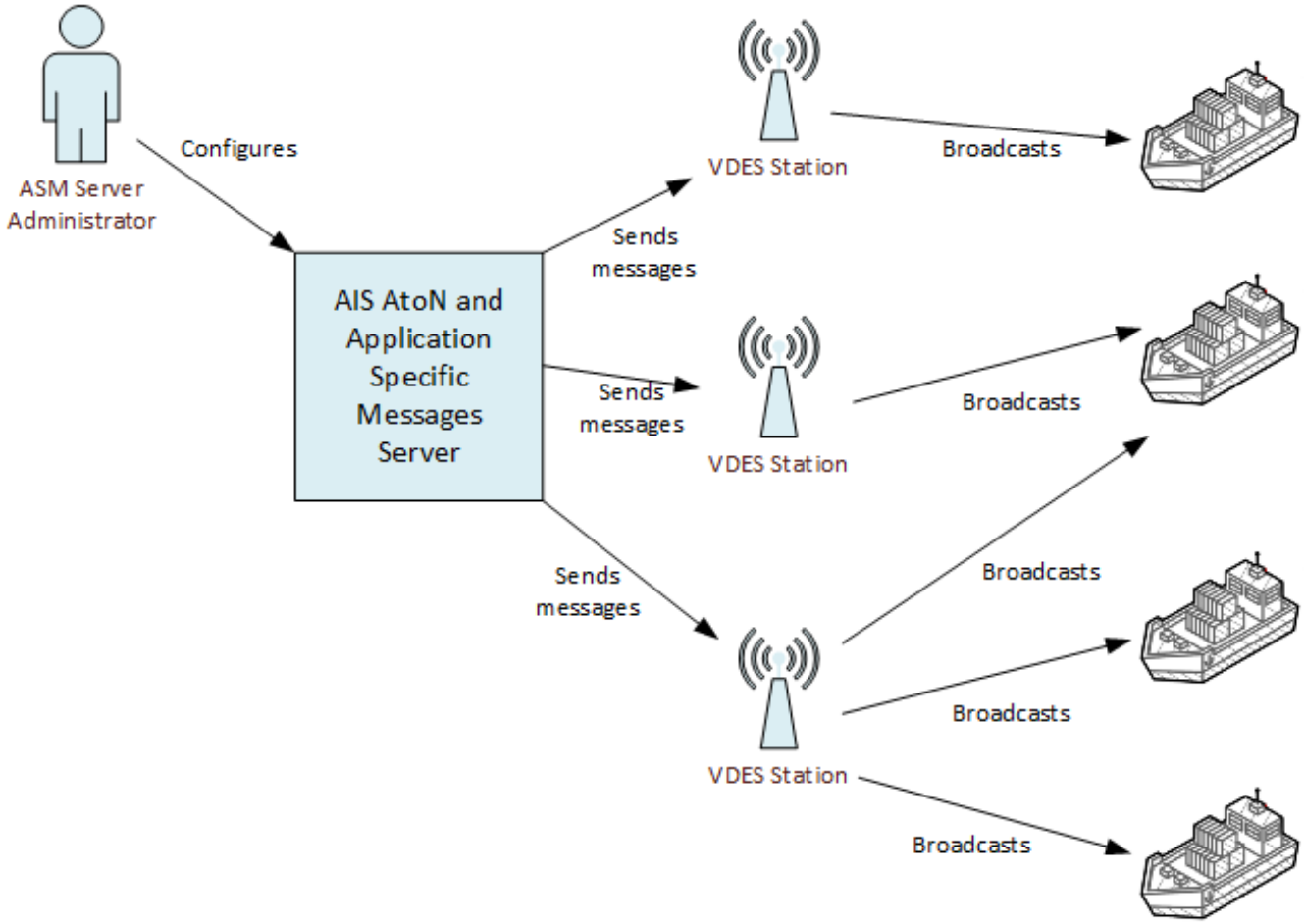

Figure 7 Use case: VDES authenticated broadcasts

6.1.2. USE CASE SUMMARY

Table 13 Use case summary

Use Case	VDES Component	Message Type	Link ID	Time Slots	Transmission Interval (s)	Time to Authentication (s)
Virtual AIS AtoN	AIS	21	N/A	2	180	60

6.2. E-NAVIGATION AUTHENTICATION REQUIREMENTS

The following requirements have been derived from the Virtual AIS AtoN use case, along with input from stakeholders and operational considerations. These requirements are intended to guide the design of VDES authentication mechanisms within the broader e-Navigation system of systems.

Table 14 E-Navigation authentication requirements

Name	Description	Priority
Source Verification	For use cases that require authentication, the system shall provide a cryptographically secure indication of the origin of received data.	Mandatory
Data Integrity	For use cases that require authentication, the system shall provide a cryptographically secure indication that the received data has not been altered or corrupted during transmission.	Mandatory
Data Freshness	For use cases that require authentication, the system shall provide a cryptographically secure indication that the received data is current and has not been replayed from a previous transmission.	Mandatory
Virtual AIS AtoN	The system shall support the authentication of Virtual AIS AtoN broadcasts in accordance with the parameters of the 'Virtual AIS AtoN' use case defined in Table 12.	Mandatory

7. PROPOSED SOLUTIONS

This section introduces candidate techniques for VDES authentication that aim to meet the requirements defined in Section 6.

In this first edition of the guideline, the focus is placed on a single method: a digital signature-based approach in which authentication information is transmitted in a separate, dedicated message over VDE-TER. Future editions may explore additional schemes, including advanced techniques such as the TESLA protocol, which offers authentication of broadcast data streams with low data overhead.

7.1. AUTHENTICATION SCHEME 1: AUTHENTICATING AIS MESSAGES USING DIGITAL SIGNATURES SENT OVER VDE-TER

7.1.1. OVERVIEW

This authentication scheme enables the verification of AIS messages by transmitting a digital signature in a follow-on message over VDE-TER.

AIS messages are transmitted without modification on the AIS 1 and AIS 2 channels. For each AIS message, a corresponding Signature Message is sent via VDE-TER. This Signature Message contains a digital signature and additional information required to verify the integrity and authenticity of the original AIS message.

Receiving applications that implement this scheme can link each Signature Message to its corresponding AIS message, validate the digital signature, and confirm that the original AIS transmission is both authentic and unaltered.

7.1.2. RATIONALE

The proposed scheme is based on the use of digital signatures, which is a well-established method for ensuring the authenticity and integrity of data, with a range of vetted algorithms and software libraries available for their implementation.

Key advantages of this scheme include:

- Backward compatibility: By transmitting authentication data separately, the original AIS message format remains unchanged. This ensures continues compatibility with legacy AIS receivers and associated systems.
- Protection of AIS: Signature Messages are transmitted over VDE-TER, preserving the limited capacity of the AIS data link for core safety-critical functions.
- Low implementation complexity: The use of standard cryptographic libraries enables straightforward integration of this scheme into existing infrastructure and software systems.

7.1.3. ACTORS AND SYSTEM COMPONENTS INVOLVED

The following components participate in the implementation and operation of Authentication Scheme 1:

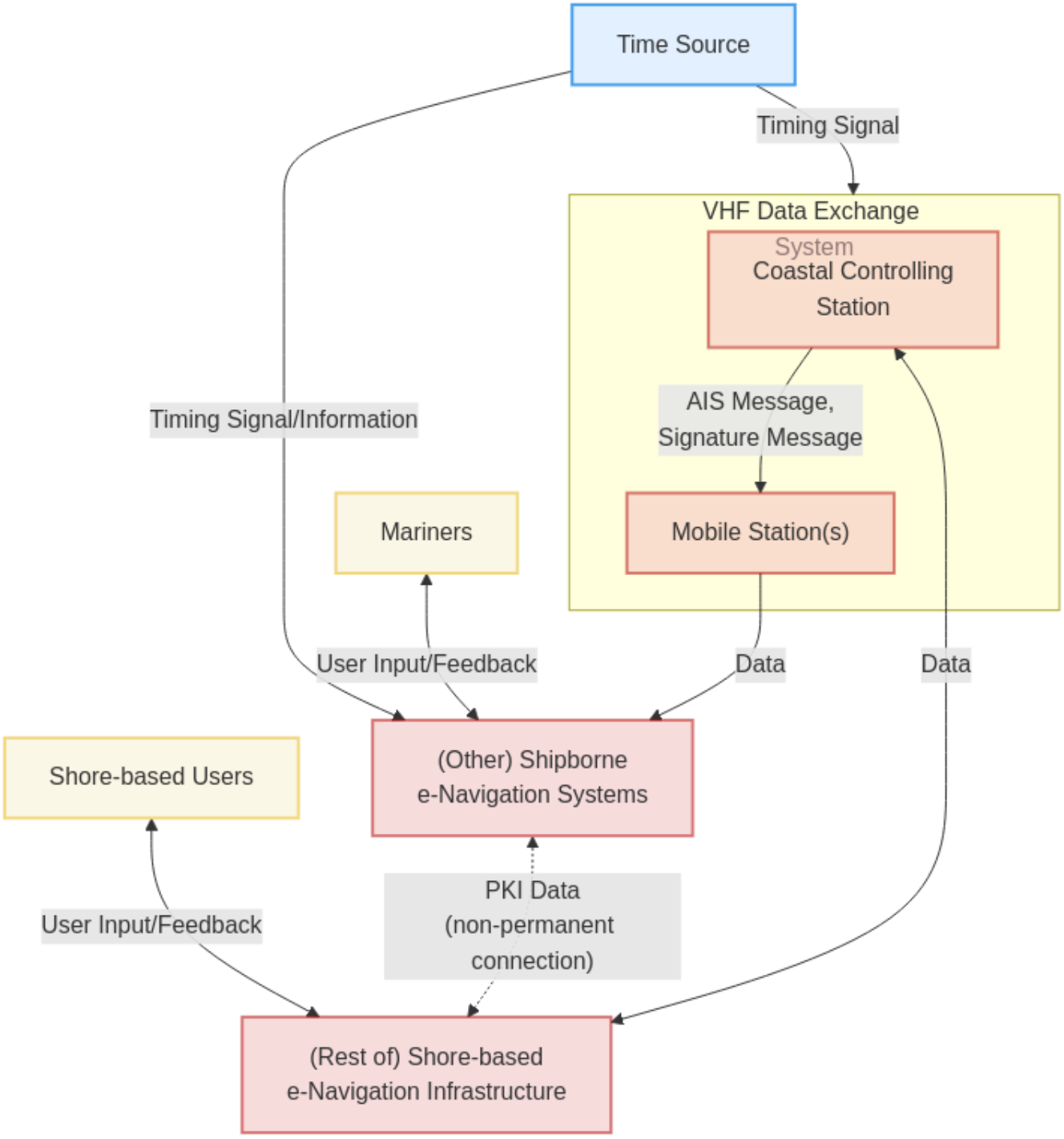

Figure 8 Actors and e-Navigation SoS components involved in proposed Authentication Scheme 1 (components shown in red are considered in scope for this solution)

7.1.3.1. Shore-based e-Navigation Infrastructure

A foundational requirement for this scheme, as any other authentication scheme based on PKC, is the existence of a **Public Key Infrastructure (PKI)**, managed under the authority of a trusted Certificate Authority (CA). The PKI enables the issuance and validation of public key certificates used in the authentication process. Further discussion of PKI considerations is provided in Section 3 and Section 5.

7.1.3.2. Shore-based Users

Shore-based users such as AtoN authorities and VTS use the Shore-based e-Navigation Infrastructure to generate a public-private key pair and a public key certificate via the PKI. Each user holds their private key securely and uses it to sign outgoing messages. The public key certificates tie each user's public key to a unique, cryptographically verifiable identity and are used by other users to verify the public key, which is then used to verify the digital signatures.

The users further use the shore-based infrastructure to set up AIS broadcasts (e.g. AIS AtoN Report), specifying whether authentication is required and which scheme is to be used.

7.1.3.3. VDES Coastal Controlling Station

Shore-based infrastructure includes VDES Coastal Controlling Stations that perform two key functions:

- Transmit AIS broadcasts on the AIS channels as configured by users.
- Transmit Signature Messages over VDE-TER, enabling cryptographic authentication of the AIS broadcasts.

7.1.3.4. VDES Mobile Station(s)

Onboard VDES Mobile Stations receive both the AIS broadcasts and the associated VDE-TER Signature Messages. These are forwarded via the presentation interface (PI) to other Shipborne e-Navigation Systems for further processing and verification.

7.1.3.5. Shipborne e-Navigation System(s)

Shipborne system(s) maintain a local store of trusted public key certificates and use them to verify the AIS data against the digital signatures received over the air. It is assumed that the local store is updated periodically with new certificate information from the shore-based infrastructure via a non-permanent, broadband connection (e.g. when the ship is in port).

7.1.3.6. Mariners

Mariners interact with shipborne system(s) to access received AIS data. When authentication is in use, mariners are provided with assurance that a given message:

- Originated from a trusted source;
- Has not been modified in transit; and
- Can be reliably attributed to the correct sender.

7.1.4. Cryptographic Algorithms

To keep authentication overheads to a minimum, it is necessary to use digital signature algorithms that keep key and signature sizes as small as possible whilst still providing a robust degree of security; examples of such include the Elliptic Curve Digital Signature Algorithm (ECDSA).

In accordance with the recommendations made in Rec. ITU-R M.2092 and IALA G1183, this scheme uses the ECDSA with the SHA-256 hash function and the secp256r1 curve. This variant of ECDSA uses 256-bit keys and produces 512-bit signatures for a security level of 128 bits (meaning that the best-known attack against the algorithm requires approximately 2^{128} operations to succeed).

7.1.5. Data Structures

7.1.5.1. Signature Message

Table 14 shows the bit structure of the application data contained in the VDE-TER Signature Message used in this scheme. The structure makes use of the VDE Protocol Format Identifier (VPFI) concept introduced in IALA Guideline *G1117 VHF Data Exchange System (VDES) Overview*, and includes fields that allow the recipient to:

1. Identify this as an authentication-related message for use with Authentication Scheme 1;
2. Link this message to the AIS message being authenticated;

3. Verify that the AIS message has not been corrupted and comes from a trusted source; and
4. Confirm that the data being received was generated within the expected time frame (i.e. it has not been replayed).

Table 15 Signature Message application data structure for Authentication Scheme 1

Field No.	Parameter	Bitcount	Decimal Value	Description
1	VPFI	16	7	VDE Protocol Format Identifier. Shall be set to 7, indicating 'Cryptographic Authentication'. See IALA G1117 for further details on the VPFI concept.
2	Message ID	6	1	Allows for multiple message types to be used within a given authentication scheme.
3	Authentication Scheme ID	8	1	Identification of the authentication scheme being used. This provides flexibility for future revisions of the schemes and extensions to address evolving security requirements. Shall be set to 1, indicating 'AIS Message Authentication over VDE-TER'.
4	AIS Message ID	6	1 to 63	The Message ID of the AIS message being signed.
5	MMSI	30	0 to $2^{30}-1$	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 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 presently output the slot number in the VSI PI sentence.
8	Timestamp	32	0 to $2^{32}-1$	Represents the 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. After 19th January 2038 03:14:07 UTC, the number is the number of seconds after this new date (wraps around); The timestamp shall be used by the system receiving this message to verify its freshness and protect against replay attacks, as follows: 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 should be discarded.
9	Signature	512	0 to $2^{512}-1$	A digital signature calculated over the concatenation of fields 1 to 8 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 that defined in Section 7.1.4
-	Total bitcount	624	-	-

7.1.5.2. Public Key Certificate

The public key certificates used in this scheme are based on the ITU-T X.509 standard and are constructed in accordance with the IALA Guideline *G1183 The Provision of Maritime Connectivity Platform (MCP) Identities*, Edition 1.1.

7.1.6. Certificate Management

When broadband connectivity is available between the Shipborne e-Navigation System(s) and the Shore-based e-Navigation Infrastructure (such as when the ship is in port), the system(s) can periodically update their local store of trusted public key certificates.

Each certificate must be validated against the corresponding CA's certificate, which is stored in the system's trusted root certificate store. The root certificate(s) are pre-installed in the system by a trusted party.

When a certificate for a new entity is received, the shipborne systems(s) should seek the user's confirmation that the entity is trusted before adding the certificate to the local store.

When the certificate information is updated, the system(s) also update a *lookup table* that maps MMSIs/Source IDs to certificates. This table allows the system(s) to quickly find the correct certificate for a given MMSI/Source ID when authenticating an AIS message. The exact method for establishing the link between certificates and AIS/VDES messages is still under discussion.

7.1.7. Message Generation and Transmission

The following steps describe the generation and transmission of a signed AIS message using this scheme:

1. The Shore-based e-Navigation Infrastructure:
    1. Gathers the data to be transmitted in the AIS message (e.g. the parameters of a Virtual AIS AtoN).
    2. Formats the data into a valid AIS message bit structure, as defined in Recommendation ITU-R M.1371 (e.g. AIS message type 21 for AtoN reports).
    3. Encapsulates the message bit structure into one or more Presentation Interface (PI) sentences requesting transmission over AIS.
    4. Inputs the PI sentence(s) to the VDES Coastal Controlling Station.
2. The VDES Coastal Controlling Station:
    1. Receives the PI sentence(s) containing the AIS message and schedules the message for transmission over AIS.
    2. Transmits the AIS message over the AIS channel(s) (unchanged from standard AIS operation).
    3. Outputs one or more PI sentence(s) to the Shore-based e-Navigation Infrastructure confirming the successful transmission of the AIS message and containing the time of transmission and the slot number used (e.g. via VSI PI sentence).
3. The Shore-based e-Navigation Infrastructure:
    1. Gathers the data required to assemble a Signature Message, including the Message ID of the AIS message being signed, the MMSI of the sender, the Channel ID of the AIS channel on which the message was transmitted and the time of transmission and slot number.
    2. Generates a digital signature for the AIS message, using the ECDSA algorithm and the user's private key. The signature is calculated over a concatenation of fields 1 to 8 of the application data structure in Table 14 and the AIS message bit structure (see the Signature field in the table for details).
    3. Assembles the application data structure defined in Table 14 and encapsulates it into one or more PI sentences requesting transmission over VDE-TER.

4. Inputs the PI sentence(s) to the VDES Coastal Controlling Station.

4. The VDES Coastal Controlling Station:

    1. Receives the PI sentence(s) containing the application data for the Signature Message, encapsulates the data into a Segment and queues the Segment for transmission over VDE-TER.

    2. Encapsulates the Segment into a VDE-TER Message, assigning it a Source ID, and schedules the message for transmission over VDE-TER.

    3. Transmits the VDE-TER Message over a VDE-TER channel.

    4. Outputs a PI sentence to the Shore-based e-Navigation Infrastructure confirming the successful transmission of the Signature Message.

7.1.8. Message Reception and Data/Signature Verification

A received AIS message can be authenticated as follows:

1. A VDES Mobile Station:

    1. Receives the AIS message transmission on the AIS channel(s).

    2. Encapsulates the received message into one or more PI sentences and outputs these to a connected Shipborne e-Navigation System. These sentences must contain the time of receipt and the slot number of the received message.

    3. Receives the Signature Message transmission on a VDE-TER channel.

    4. Encapsulates the received message into one or more PI sentences and outputs these to a connected Shipborne e-Navigation System. These sentences must contain the time of receipt of the message.

2. The Shipborne e-Navigation System:

    1. Receives the PI sentence(s) and extracts the encapsulated message and metadata (time of receipt, slot number).

    2. If the received message is an AIS message, the system stores it in a cache, along with a record of the time of receipt and slot number.

        At the same time, the system forwards the AIS message for further processing and/or display, marking it as Unverified.

    3. If the received message is a Signature Message, the system:

        1. Compares the Timestamp in the Signature Message with the time of receipt of said message.

        2. If the system determines that the Timestamp is more than 60 seconds before the time of receipt of this Signature message then this Signature message should be discarded and no further action is taken.

        3. Otherwise, the system:

            1. Searches the cache for an AIS message that matches the AIS Message ID, MMSI, Channel ID, Timestamp and Slot number contained in the Signature Message.

            2. If a matching AIS message is found, the system:

                1. Concatenates fields 1 to 8 of the Signature Message with the AIS message bit structure. The bits corresponding to the AIS message shall form the least significant bits of the concatenated data.

2. Fetches the public key certificate corresponding to the MMSI/Source ID in the Signature Message from the local store, making use of the certificate lookup table (see Section 7.1.6).
3. Verifies the concatenated data using the ECDSA signature verification algorithm, the public key extracted from the certificate and the digital signature from the Signature Message (Cryptographic/Signature Verification).
4. If the verification is successful, the system releases the AIS message for further processing and/or display, marking it as *Authenticated*.
5. If the verification fails, the system releases the AIS message for further processing and/or display, marking it as *Authentication Failed*.

3. If no matching AIS message is found, the system discards the Signature Message.

4. Cached AIS messages that are not matched with a Signature Message within 60 seconds are deleted from the cache.

7.1.9. Message Processing and Display Policies

Shipborne e-Navigation System(s) can apply different policies to the processing and/or display of AIS messages based on their authentication status - for example:

- Authenticated: The AIS message is displayed to the user with an indication that the data has successfully been authenticated.
- Failed Authentication: A Signature Message was received and matched to the AIS message; however, verification of the digital signature failed. This may indicate message corruption or a potential security issue. The message may still be displayed but should be clearly flagged as 'authentication failed', and appropriate alerts or warnings may be presented to the user.
- Unverified: The AIS message is displayed to the user without any indication of its authenticity, as is presently the case with all AIS messages.

7.1.10. Example Implementation

The Research and Development team at the General Lighthouse Authorities of the UK and Ireland (GRAD) has implemented a version of this authentication scheme within their prototype e-Navigation Service Architecture - a software framework for the provision of digital services in accordance with IMO, IALA and IEC guidelines and standards. The GRAD implementation integrates with the Maritime Connectivity Platform (MCP) and has successfully been tested in several over-the-air demonstrations of authenticated Virtual AIS AtoN provision.

For more information on the GRAD implementation, deployment options and instructions for contributing to the project, please refer to the GRAD eNav-Config repository on GitHub.

The code for generating and verifying digital signatures is available in the eNav-CKeeper repository.

Sample application code for verifying digitally signed AIS AtoN Report messages using the GRAD libraries can then be found in their ais repository on GitHub.

It should be noted that the GRAD implementation is a research prototype and is not intended for operational use. The implementation may not be fully aligned with this guideline as it is subject to ongoing development and testing.

8. DISCUSSION

8.1. DATA LINK CAPACITY CONSIDERATIONS

A key consideration in evaluating the feasibility of VDES authentication schemes is their impact on the overall data link load. In particular, it is important to assess how many additional time slots are consumed by authentication-related transmissions and how this compares to the available link capacity.

To support this assessment, the following discussion outlines the data link capacities of the relevant VDES components. This contextual information is essential for understanding the operational implications of introducing authentication messages into the system.

Subsequent analysis in this section will quantify the time slot usage of candidate authentication schemes under specific use case scenarios, enabling an informed comparison between security benefits and data link costs.

8.1.1. AIS

As established in Section 2, AIS provides a maximum of 2,250 time slots per minute, with transmissions spanning one to five slots. These time slots can be reused across different frequency channels. Most existing AIS applications operate on the AIS 1 and AIS 2 channels, with an additional two channels available for long-range tracking.

In congested areas, the AIS data links are already heavily utilized for core AIS functions (such as vessel position reporting), leaving little spare capacity for extra data transmission. For this reason, the use of AIS for authentication purposes is discouraged, as it would further strain the AIS data links.

8.1.2. VDE-TER

Similar to AIS, VDE-TER offers a maximum of 2,250 time slots per minute, with transmissions always taking up one slot.

In simplex mode, one 100 kHz-bandwidth channel (Link ID 17 or 19) is used for shore-to-mobile, mobile-to-shore and mobile-to-mobile communications. The 100 kHz bandwidth can be split into four channels (Link ID 11), each 25 kHz wide, with up to 2,250 slots per minute available in each channel (albeit with a lower per-slot data capacity).

In duplex mode, one 100 kHz-bandwidth channel is used for shore-to-mobile and mobile-to-mobile communications, and another 100 kHz-wide channel is available for mobile-to-shore communications. These channels can each be split into four 25-kHz bandwidth channels.

It should be noted that the number of time slots per minute available to a station on a given VDE-TER channel will in practice be lower than the 2,250 maximum due to factors such as:

- The need to share time slots among neighbouring stations (in particular, where the 100 kHz bandwidth channels are used and sharing in frequency is not possible); and
- The concepts of logical channels and TDMA channels (not discussed here in detail) that further restrict the number of slots available for data exchange by assigning them to specific uses.

8.2. ASSESSING AUTHENTICATION SCHEME 1 (AIS AUTHENTICATION USING DIGITAL SIGNATURES OVER VDE-TER)

8.2.1. USE CASES AND SCENARIOS CONSIDERED

To present an illustrative example, we consider applying Authentication Scheme 1 to the Virtual AIS AtoN use case introduced in Section 6. Further use cases may be included in a future edition of this guideline.

In this example, we consider a scenario where 16 Virtual AIS AtoN are active in a service area. When marking a new hazard, four Virtual AIS AtoN are typically used to mark the north, south, east and west boundaries of the hazard.

Limiting the number of active transmissions to 16 therefore allows for the marking of up to four hazards within the footprint of the transmitting station, while ensuring a negligible impact on the AIS data link loading and avoiding display clutter.

8.2.2. DATA LINK LOAD ANALYSIS

To determine the number of time slots required for authentication, we apply the procedure outlined at the end of Section 2.3.4.

From Table 14 in Section 7, we see that the data (including the appropriate VPFI) to be sent in each Signature Message is 624 bits in size.

This results in a VDE-TER segment of 624 + 32 = 656 bits in size.

From Table 7 in Section 2, we see that:

- If Link ID 11 (25 kHz bandwidth channel) is used to transmit the Signature Message, then the data (segment) to be transmitted exceeds the maximum payload size of the single-slot short data message (304 bits). Consequently, multiple slots must be allocated for a data session. From Table 7, we determine that three fragment messages are required to transmit the 656-bit segment.
- If Link ID 17 or 19 (100 kHz bandwidth channel) is used, the Signature Message data will fit into a single short data message, thereby avoiding the need for a data session. It should, however, be noted that these Link IDs will likely provide a shorter range than Link ID 11 or the AIS on which the data being authenticated is transmitted.

As discussed in Section 6, AIS AtoN Reports are typically transmitted in 180-second (3-minute) intervals (see Table 12). Since our scenario involves 16 active Virtual AIS AtoN transmissions, we can calculate the number of time slots required for authentication as follows:

- For Link ID 11: 16 * 3 / 3 = 16 slots will be used per minute for Signature Message transmission.
- For Link ID 17 or 19: 16 * 1 / 3 = 6 slots will be used for authentication in each frame.

8.2.3. CONCLUSIONS

The analysis presented in this section demonstrates that applying Authentication Scheme 1 to the Virtual AIS AtoN use case is expected to have minimal impact on the loading of the VDE-TER data link, irrespective of the Link ID selected for transmission.

It should, however, be noted that the use of Link ID 11, favoured for its longer range, may require a larger percentage of slots in each frame to be allocated for use by the transmitting station, which may impact the availability of slots for other users in the area.

Overall, the proposed authentication scheme is considered feasible from a data link perspective when applied to the Virtual AIS AtoN use case.

9. NEXT STEPS

To support the continued development, validation and eventual adoption of VDES authentication solutions, the following next steps are recommended:

1. Implementation and testing:

   IALA members are encouraged to integrate the proposed authentication scheme into their existing e-navigation test environments and to report findings and lessons learned to the IALA Digital Technologies Committee. These insights will be instrumental in refining the proposed schemes and guiding future development.

2. Expansion of use cases and techniques:

Future editions of this guideline should expand the range of use cases, including those involving higher message volumes. In parallel, more advanced authentication schemes may be explored - such as those based on the TESLA protocol - or the adoption of quantum-safe cryptography in preparation for long-term security needs.

3. Operational performance requirements:

   The set of authentication requirements may be strengthened through the inclusion of operational performance parameters, such as availability and continuity of service.

   These parameters will help ensure that authentication mechanisms meet safety-critical expectations.

4. Technical topics for further development:

   A number of technical matters must be addressed in support of widespread and standardised adoption. These include:

   - Reception metadata output: Define a method for outputting the time of reception and slot number of received messages by VDES mobile stations (such as through the VSI PI sentence).
   - Association of certificates with AIS/VDES messages: Develop a standardised method for linking certificates to the VDES messages they authenticate. Key considerations include:
     - Whether a certificate identifier should be included in the Signature Message or in a dedicated message.
     - Whether to link the certificate to the MMSI of the AIS message or the MMSI/Source ID of the Signature Message.
   - Collaboration between DTEC Working Group 1 and Working Group 3 is recommended to ensure alignment with related IALA efforts and documents.

5. Development of a standardisation roadmap:

   A structured roadmap should be developed to define the steps required for:

   - Standardisation of VDES authentication schemes;
   - Wider implementation across the maritime domain; and
   - Alignment with ongoing IALA, ITU, and IEC initiatives.

10. DEFINITIONS

The definitions of terms used in this Guideline can be found in the *International Dictionary of Marine Aids to Navigation* (IALA dictionary) and were checked as correct at the time of going to print. Where conflict arises, the IALA Dictionary should be considered as the authoritative source of definitions used in IALA documents.

Authentication (from Greek: αὐθεντικός *authentikos*, “real, genuine”, from αὐθέντης *authentes*, “author”) is the act of proving an assertion, such as the identity of a computer system user [13].

11. ABBREVIATIONS

AIS	Automatic Identification System
GNSS	Global Navigation Satellite System
VDES	VHF Data Exchange System
VHF	Very High Frequency

12. REFERENCES

[1] International Organization for Marine Aids to Navigation (IALA), "VHF data exchange system (VDES) overview," Guideline 1117. Available: https://www.iala-aism.org/product/g1117/.

[2] International Maritime Organization (IMO), "E-navigation." Available: https://www.imo.org/en/OurWork/Safety/Pages/eNavigation.aspx.

[3] International Telecommunication Union (ITU), "Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band," Recommendation ITU-R M.1371-5, Feb. 2014.

[4] International Telecommunication Union (ITU), "Technical characteristics for a VHF data exchange system in the VHF maritime mobile band," Recommendation ITU-R M.2092-1, Feb. 2022. Available: https://www.itu.int/rec/R-REC-M.2092-1-202202-I/en.

[5] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," *CryptoBytes*, vol. 5, no. 2, pp. 2–13, 2002, Available: https://people.eecs.berkeley.edu/~tygar/papers/TESLA_broadcast_authentication_protocol.pdf

[6] F. Lázaro and R. Raulefs, "An authentication concept for VDES r-mode," International Association of Marine Aids to Navigation; Lighthouse Authorities, Input Paper ENAV28-5.1.3.1, Sep. 2021.

[7] F. Lázaro, R. Raulefs, and M. Wirsing, "Verfahren zur authentifizierung einer sendeeinheit durch eine empfängereinheit," German Patent Application DE 10 2021 119 891.7, 2021

[8] F. Lázaro, R. Raulefs, H. Bartz, and T. Jerkovits, "VDES r-mode: Vulnerability analysis and mitigation concepts," *Satell Commun Network*, vol. 41, no. 2, pp. 178–194, Mar. 2023, doi: 10.1002/sat.1427. Available: https://onlinelibrary.wiley.com/doi/10.1002/sat.1427.

[9] G. Wimpenny, F. Lázaro, J. Šafář, and R. Raulefs, "A pragmatic approach to VDES authentication," *NAVIGATION: Journal of the Institute of Navigation*, vol. 72, no. 1, p. navi.681, 2025, doi: 10.33012/navi.681. Available: http://navi.ion.org/lookup/doi/10.33012/navi.681.

[10] National Cyber Security Centre, "Preparing for quantum-safe cryptography," 2020. Available: https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography.

[11] Bundesamt für Sicherheit in der Informationstechnik, "Kryptografie quantensicher gestalten - grundlagen, entwicklungen, empfehlungen," 2021. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.pdf.

[12] S. Bober, W. Haupt, and N. Braunroth, "Implementing digital aids to navigation in european inland navigation," in *Proc. 20th IALA conference*, Rio de Janeiro, Brazil, May 2023.

[13] "Authentication," *Wikipedia*. Feb. 13, 2024. Available: https://en.wikipedia.org/w/index.php?title=Authentication&oldid=1206921340.