|  |
| --- |
| IALA Guideline |

Gnnnn

VDES Authentication Techniques

Edition x.x

Date (of approval by Council)

urn:mrn:iala:pub:gnnnn

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

|  |  |  |
| --- | --- | --- |
| Date | Details | Approval |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**No table of contents entries found.**

List of Tables

**No table of figures entries found.**

List of Figures

***No table of figures entries found.***

# Introduction

* High-level introduction to VDES and the need for authentication in the maritime domain
* Document purpose
* Scope

# VDES Overview

* VDES architecture
* Summary of pertinent technical characteristics

# Possible Attack Vectors and Impact on Operations

* Spoofing GNSS and the need for resilient PNT
  + See [IALA G1180 on Resilient PNT](https://www.iala-aism.org/product/g1180-resilient-pnt/)
* Spoofing VDES messages
  + Consider different layers of the protocol stack
  + TBB authentication - perhaps IALA could be the CA
  + Consider different applications
* Other
* Impact on operations, incl. examples of past incidents

# Fundamental Concepts of Cryptographic Authentication

* Distinction between authentication and encryption
* Symmetric vs. asymmetric cryptography
* Digital signatures
* TESLA (Timed Efficient Stream Loss-tolerant Authentication)?
* Public Key Infrastructure
* Certificate Authorities

# Challenges to VDES Authentication

* Backwards compatibility requirements
* Low data rate
* Key and certificate management
* Quantum computing and implications for the long term
* Export control restrictions on cryptographic technologies (probably not an issue for VDES as this is for public/non-military use)

# VDES Authentication Requirements

* Requirements at the e-navigation system/infrastructure level (consider specific applications / use cases / services and any regulatory requirements)
* Reference e-navigation system/infrastructure architecture
* Derived requirements for VDES and related system elements
* Use Case Champions
  + Stefan Bober - Virtual AIS AtoN
    - [Implementing Digital Aids to Navigation Information in European Inland Navigation](source/guideline/../../references/Bober_et_al-2023-Implementing_Digital_Aids_to_Navigation_Information_in_European_Inland_Navigation.pdf) [1]
  + Jean-François Coutu - [AIS AtoN and Application Specific Message Shore-to-ship Broadcast](source/guideline/../images/use_case_vdes_authentication_broadcasts.vsdx)
  + Ronald Raulefs - R-Mode
  + Cato Eliassen - CySiMS 1 and 2 projects produced a pilot service which was a basis for an input paper to IMO FAL. For details, see:
    - <http://cysims.no/>
    - <https://doi.org/10.1088/1757-899X/929/1/012017>
  + Yi Jiang - Navigation System Monitoring Status (shore to ship)
  + Stefan Pielmeier - Maritime Messaging Service (MMS) related use cases

# Potential Solutions

* Overview of solutions
* Detailed description of each candidate VDES authentication technique
* Anticipated interactions with non-VDES system elements, e.g. to support key and certificate management (Maritime Connectivity Platform)
  + IALA DTEC WG1 is already working on a guideline explaining how to set up a PKI.

# Discussion

* Assessment of each solution against the requirements
* Trade-offs

# Next Steps

* Recommendations for further work (short-term actions, long-term strategies, further research)
  + IMO is a Certificate Authority, already provides a PKI for LRIT. For details, see [IMO MSC.1/Circ.1376/Rev.5](https://wwwcdn.imo.org/localresources/en/OurWork/Safety/Documents/LRIT/1376-Rev.5.pdf)
* Feedback mechanism

# Definitions

The definitions of terms used in this Guideline can be found in the *International Dictionary of Marine Aids to Navigation* (IALA dictionary) at <http://www.iala-aism.org/wiki/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 [2].

# Abbreviations

| Abbreviation | Description |
| --- | --- |
| AIS | Automatic Identification System |
| GNSS | Global Navigation Satellite System |
| VDES | VHF Data Exchange System |
| VHF | Very High Frequency |

# References

[1] 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.

[2] “Authentication,” *Wikipedia*. Feb. 13, 2024. Available: <https://en.wikipedia.org/w/index.php?title=Authentication&oldid=1206921340>. [Accessed: Feb. 20, 2024]