Input paper: [[1]](#footnote-1) DTEC2-5.2.3.9

Input paper for the following Committee(s): Purpose of paper:

**□** ARM **□** ENG **□** PAP X Input

X DTEC **□** VTS **□** Information

Agenda item [[2]](#footnote-2) n.n

Technical Domain / Task Number 2 …………………………………

Author(s) / Submitter(s) GLA R&D (GRAD)

Draft New Guideline on VDES Authentication Techniques

# Summary

## Purpose of the document

This document describes the intended approach for the development of a new IALA Guideline on VDES Authentication Techniques. It provides a high-level overview of the content of the proposed guideline and seeks feedback from the Committee.

## Related documents

IALA Recommendation 1007 [1]

IALA Recommendation 1017 [2]

IALA Guideline 1117 [3]

IALA Guideline 1158 [4]

# Background

During IALA DTEC1, GRAD was assigned the task of coordinating the development of a new IALA Guideline on VDES Authentication Techniques. This guideline aims to provide the maritime community with guidance on the use of cryptographic authentication techniques to ensure the integrity and authenticity of VDES communications.

# Discussion

## Proposed Approach

### Document Format

We intend to write the document in Markdown, a plain text format that facilitates online collaboration and version control. Markdown offers a lightweight syntax that supports features such as cross-referencing and LaTeX-style mathematics, making it a suitable choice for technical documentation. Its use also allows for automatic conversion to various document formats, including ‘.docx’ and ‘.pdf’. To ensure consistency in formatting, we have created a template that aligns with the IALA Style Guide.

### Version Control

We use Git/GitHub for version control. The ‘main’ branch in our GitHub repository serves as the single source of truth for our documents, preventing potential confusion due to multiple document versions in circulation. Documents can be previewed on GitHub at any time, and updated ‘.docx’ files are automatically generated and made available whenever new content is merged into the ‘main’ branch.

### Contribution Process

Contributors are invited to propose changes by submitting ‘pull requests’ on GitHub at their convenience. Contributions via GitHub are preferred for efficiency and traceability. Change proposals will be processed during official meetings of IALA DTEC Working Group 3. This procedure ensures that all changes are reviewed and agreed upon by the working group members before they are incorporated into the official document.

## Proposed Document Structure

We propose the following structure for the guideline as a starting point for discussion:

1. Introduction

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

1. VDES Overview

* VDES architecture
* Summary of pertinent technical characteristics

1. Possible Attack Vectors and Impact on Operations

* Spoofing GNSS and the need for resilient PNT
* Spoofing VDES messages
* Other
* Impact on operations, including examples of past incidents

1. 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

1. Challenges to VDES Authentication

* Backwards compatibility requirements
* Low data rate
* Key and certificate management
* Quantum computing and implications for the long term

1. 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

1. Potential Solutions (may be multiple sections)

* Overview of solutions
* Detailed description of each candidate solution
* Anticipated interactions with non-VDES system elements, e.g. to support key and certificate management (Maritime Connectivity Platform)

1. Discussion

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

1. Next Steps

* Recommendations for further work (short-term actions, long-term strategies, further research)
* Feedback mechanism

1. Definitions
2. Abbreviations
3. References
4. Annexes

* Case studies and examples of implementation

# References

[1] International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA), ‘VHF Data Exchange System (VDES) for Shore Infrastructure’, St-Germain-en-Laye, France, Recommendation 1007 Ed. 1.1, Jun. 2017. Accessed: Feb. 23, 2024. [Online]. Available: https://www.iala-aism.org/product/r1007/

[2] International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA), ‘Resilient Position Navigation and Timing (PNT)’, St-Germain-en-Laye, France, Recommendation R1017 Ed. 1.1, Dec. 2018. Accessed: Feb. 23, 2024. [Online]. Available: https://www.iala-aism.org/product/r1017/

[3] International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA), ‘VHF Data Exchange System (VDES) Overview’, Guideline 1117 Ed. 3, Dec. 2022. Accessed: Aug. 29, 2023. [Online]. Available: https://www.iala-aism.org/product/g1117/

[4] International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA), ‘VDES R-Mode’, St-Germain-en-Laye, France, Guideline 1158 Ed. 1.1, Dec. 2020. [Online]. Available: https://www.iala-aism.org/product/g1158-vdes-r-mode/

# Action requested of the Committee

Committee members are requested to review the proposed approach and provide feedback on the structure and content of the guideline to the task leader.

Individuals interested in contributing to the development of the guideline are encouraged to send their GitHub user name to [jan.safar@gla-rad.org](mailto:jan.safar@gla-rad.org) to receive access to the GitHub repository containing the guideline’s source.

1. Input document number, to be assigned by the Committee Secretary [↑](#footnote-ref-1)
2. Leave open if uncertain [↑](#footnote-ref-2)