 Input paper: [[1]](#footnote-1) ENAV18-11.10

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

**□** ARM **□** ENG **□** PAP **☒** Input

**☒** ENAV **□** VTS **□** Information

Agenda item [[2]](#footnote-2) 11

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

Author(s) / Submitter(s) Hannu Peiponen, Antti Kukkonen / Furuno Finland Oy

Integrity monitoring and authentication for VDES

Pre-Distributed Public Keys

# Summary

This paper proposes a method for delivery of keys required for authentication of application data transmitted over VHF Data Exchange System (VDES).

## Purpose of the document

IALA ENAV Committee WG3 Telecommunications is invited to consider and if found feasible, implement the proposed method into the technical annex of draft IALA guideline on VDES.

## Related documents

No related documents.

# Background

The IALA VDES Workshop organized in Tokyo 15-19 February 2016 noted that Cyber Security is an important matter to be considered for the VDES and further considered that it is necessary to agree on a mechanism for authenticating the source of information that is transmitted by using the VDES.

The workshop further developed a draft technical annex for the envisioned future IALA guideline on VDES. This draft technical annex contains a proposal for the provision of means for Cyber Security in form of both PKI and using certificates in building the line of trust.

# Discussion

While appreciating the discussion and output at the IALA VDES Workshop in February 2016, as a continuation of the discussion, we propose to amend the method of authentication by implementing use of pre-distributed public keys.

Target of this proposal is authentication of payload for VDES related applications transferred over the VDES. Authentication of the Bulletin Board of the VDES is a separate issue – it may need or not need authentication. If the Bulletin Board needs authentication, it could be based on ideas introduced in this document or on some other idea.

The particular motive for our suggestion is to keep the standard method of authentication compatible with all methods of existing and future marine communications.

In detail, to our experience an automatic on-line check for a chain of trusted certificates may become restrictive from the compatible communication methods point of view due to the related latency issues typical for maritime communications between ship and shore.

The mechanism of authentication by using pre-distributed public keys as proposed in this paper has been proven feasible in the distribution of Electronic Nautical Charts (ENC), including online updates (See IHO S-63).

The application of the proposed method for Shore-to-Ship, Ship-to-Shore and Ship-to-Ship transactions is briefly described in following Figures 1 to 4.

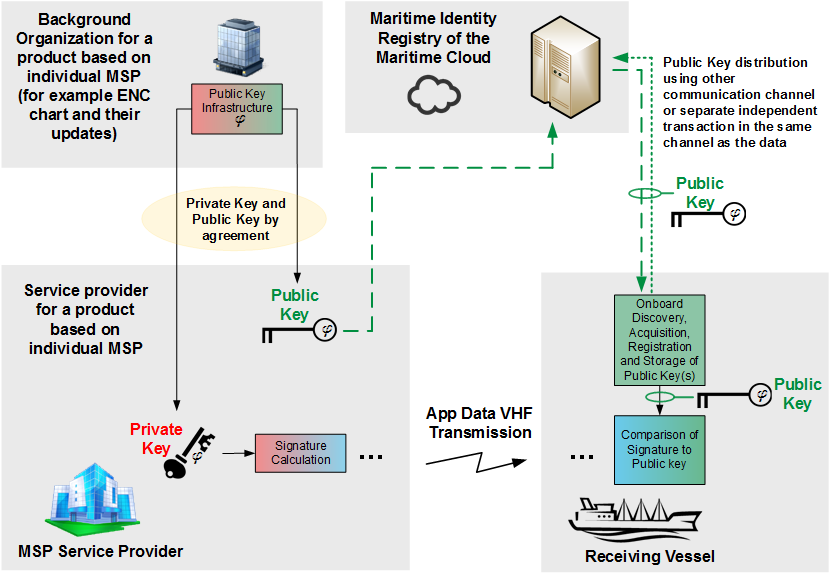


Figure 1 Public Key pre-distribution for authenticating Shore-to-Ship Official MSP transaction application data

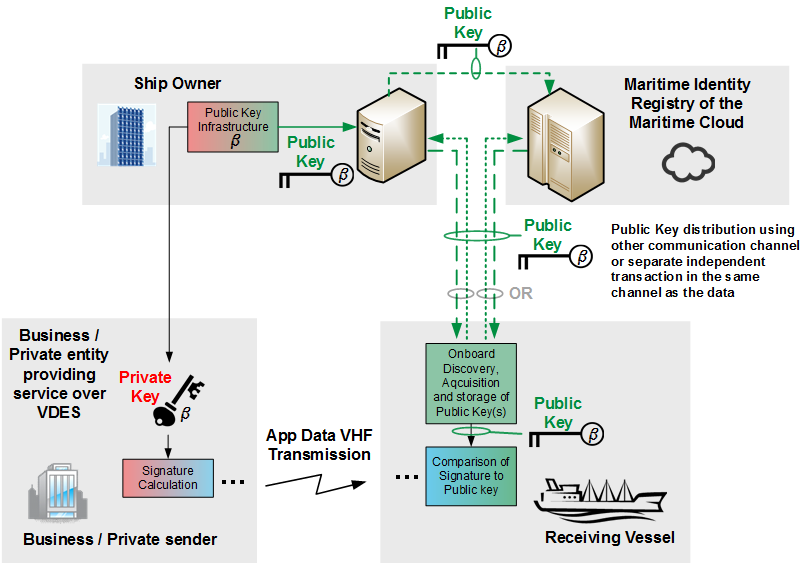


Figure 2 Public Key pre-distribution for authenticating Shore-to-Ship business / private transaction application data

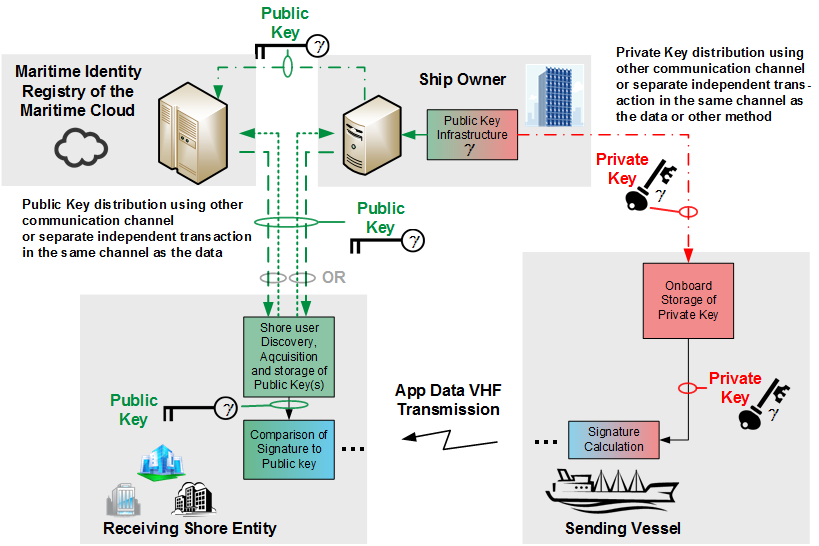


Figure 3 Public Key pre-distribution for authenticating Ship-to-Shore application data

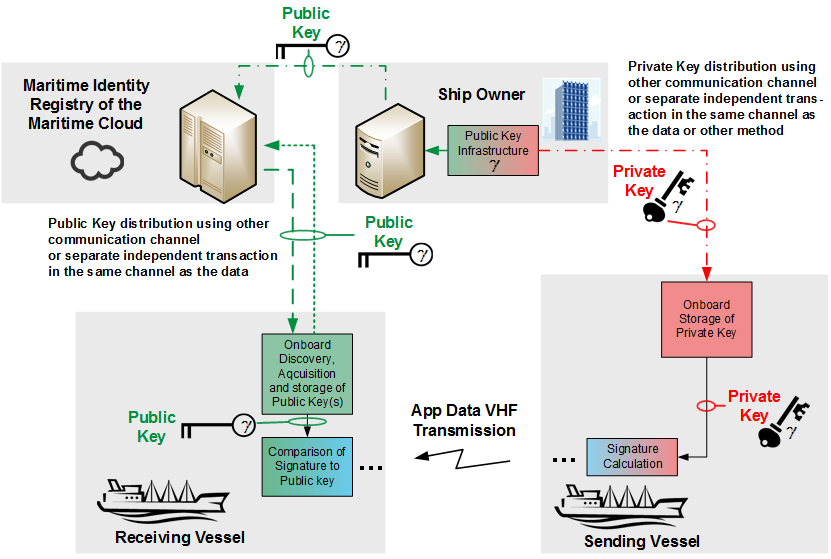


Figure 4 Public Key pre-distribution for authenticating Ship-to-Ship application data

**Properties:**

(1) Pre-distribution of Public Key(s) can be carried out by any standard communication means including VDES. If VDES is used for transfer of the keys, then the related communication session should be arranged separately from transfer of the payload. Adopting a standardized electronic key-interchange format could assist in inputting the Public Keys to ship equipment. Alternatives for a distribution format could be at least IHO S-63 pub, X.509 or email signature. One obvious source of the pre-distribution of the public key(s) could be the Maritime Identity Registry of the Maritime Cloud.

(2) If the keys in use are compromised, a new Public Key could be transmitted by using any available standard marine communications method. Data consumer application would just recognize that installed key no longer matches to the signature of the received data and would prompt user about the detected discrepancy. User could then have option to temporarily trust received data, install new key or discard the received data. Application could offer a wizard for requesting new key and installation of it.

**Recognized further items to discuss/develop**

(a) Adoption for different Public Keys of different instances requires simultaneous handling of multiple public keys by the shipborne VDES related applications. This detail should be included into the IALA Guideline on user requirements for VDES related applications.

(b) There should be an easy way to input the Public Key, received by other means than VDES, into VDES related application in any shipborne equipment. This could belong to a function of registering VDES related application for a service. Also this detail should be included into the IALA Guideline on user requirements for VDES related applications.

* For example every ECDIS is required to have two independent methods for entering the Public Key for ENC charts and their updates. First method is based on a file in "IHO S-63 .pub"-format or in X.509-format. Second method is based on manual input of the character string representing the Public Key. The second method can be used if the first method is not possible, the related text string could have been received by any method supporting text (for example Navtex, email, voice, etc.)

(c) Each instance providing VDES related application services could either establish own PKI or agree to use some existing PKI provided for example by the competent international body (for example IHO, IALA, etc.), by an administration of the country the service instance is registered to or by a ship owner (especially for use cases when a ship is source of data). Also this detail should be included into the IALA Guideline on user requirements for VDES related applications.

* For example IHO has provided Public Key infrastructure for all publishers of ENC charts and their updates. The Private Key have been provided by IHO for data source based on written agreement between data source and IHO. The Public Key has been available for downloading from web-page of IHO. Typically ECDIS manufacturers have preloaded this Public Key into their ECDIS before delivery to the customers.

# References

1. IHO Publication S-63: IHO Data Protection Scheme, Ed 1.2.0, Jan 2015

# Action requested of the Committee

The Committee is requested to:

1. Note the information within this paper,
2. Discuss the matter at an appropriate time and
3. Include the proposed into the IALA documentation if so considered by the discussion.

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