Input paper: [[1]](#footnote-2) DTEC5-6.2.3.6

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

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

**X** DTEC **□** VTS **□** Information

Agenda item [[2]](#footnote-3) n.n

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

Author(s) / Submitter(s) Stefan Pielmeier and CML

Extending VDES Authentication Support

# Summary

This paper raises proposed additions to ITU-R M.2092 and IALA Guideline G1117 to support authentication on VDES.

## Purpose of the document

This paper proposes mechanisms to address various aspects of VDES authentication support, including fingerprinting to identify certificates, distribution of public key certificates and a method to optionally sign and VDE-TER or VDE-SAT message.

Various parties contributed to the concepts raised in this paper. The objective of this paper is not to promote one implementation over the other, but to encourage open dialog in the IALA working group, to ensure that VDES authentication is viable and practical.

## Related documents

1. ITU-R M.2092-1
2. IALA Guideline G1117

# Background

As defined in [1], the Terrestrial Bulletin Board (TBB) and Satellite Bulletin Board (SBB) shall utilise a cryptographic signature so that the mobile unit can verify that that the TBB and SBB was received from a trusted source. To authenticate the signed message the mobile unit requires a valid public key. As defined in [1], ITU-R X.509 public key certificates are used to manage and authenticate public keys.

This paper describes how certificates can be managed in VDES and proposes a number of additions in [1] and [2] to support this.

Due to the fact the a VDES mobile unit needs to support authentication of the TBB and SBB, it needs to support all the verification and certificate management functionality on the hardware. As this functionality is already supported by the unit, this paper also proposes a further addition to [1], that will support the authentication of any data over VDE-TER and VDE-SAT as required. This mechanism further supports the authentication requirements of the IMO VDES performance standard.

# Discussion

## Identifying public key certificates

When a VDES unit receives a signed bulletin board, it shall authenticate it by use of the public key that matches the private key used for signing. That public key is contained in a public key certificate, which needs to be published by the organization that signs the bulletin board and is transferred to the VDES unit either by MKD, PI or VDL through the G1117 mechanism proposed in section 3.2. Each certificate loaded on the VDES unit is authenticated according to the methods defined in ITU-R X.509, before it shall be taken into use.

When receiving a signed TBB or SBB message, the correct public key certificate must be used to authenticate the message. Various mechanisms have been evaluated to select the correct certificate to use. As a certificate can expire, it should be feasible to load the next certificate for use before the previous one expires, thus supporting continuous operation. As there should be an overlap where two certificates are valid, it is proposed that each signed message provides an indication of the certificate to use, to verify the message.

It is proposed to define a short fingerprint to be sent with every signed message, to identify the certificate that should be used to verify the signed message. See SP-1 . This mechanism is only used as a lookup to identify a certificate; it is not used to indicate that a certificate is authentic or not. Once identified, the certificate can be used to authenticate the received signed message.

Using a short 6-byte fingerprint, does imply that there is a very small but existing possibility for two certificates to result in the same fingerprint. In this case, both certificates should be used for verification, and the message can be verified if one certificate passes.

If a VDES unit does not have a certificate matching the fingerprint, it can either be requested from external equipment via the PI, or it can be requested over the VDL, using the mechanism described below.

## Public key certificate distribution over the VDL

As defined in [2], VPFI 0 has been allocated to the distribution of public key certificates and certificate revocation lists (CRL). Four new messages have been proposed in CML-2:

* Certificate Report
* Certificate Request
* Certificate Revocation List Report
* Certificate Revocation List Request

These messages support the process of requesting and sharing public key certificates and CRLs, using its fingerprint for identification.

A root certificate can only be loaded by an authorised installer via the PI. Any intermediate or end public key certificates must first be authenticated by the root certificate or a subsequent intermediate certificate before it can be used. To support identification of the relevant certificates in a chain of trust, a Certificate Report shall include the fingerprint of the issuer certificate directly above it. This allows all certificates to be identified in the chain of trust.

A shore station or satellite may broadcast Certificate Report or Certificate Revocation List Report at regular intervals ensuring mobile units are using the latest credentials. A CRL is associated with a specific certificate, indicating derived certificates that should be revoked. Due to this association the issuer certificate signature is reported along with the CRL. It is also used with the CRL request to uniquely identify the correct CRL.

## VDES authentication support for other messages

Since the VDES mobile hardware needs to support certificate management and exchange, to authenticate the TBB and SBB, this functionality may be extended to support authentication of other VDES message as well. It is proposed to modify the segmentation header, to provide the optional functionality of signing the segment if requested by the PI, as detailed in CML-1.

To ensure unsigned segments remain size compatible with the current definition in [1], it is proposed to reduce the existing 16 bit “sequential ID” to 14 bits and allocating the top 2 bits to indicate the segmentation header type. The default segment type (0) aligns with the current segment header in size defined in [1]. When a signed segment type (1) is required, the segment is appended with a Timestamp, Fingerprint and Signature after the payload.

When calculating the signature, the Source MMSI and Destination MMSI is prepended to the input data. This is only done for the calculation, the Source MMSI and Destination MMSI is not transmitted again, as it is already defined in the fragment headers. This mechanism ensures the intended source and destination entities are authenticated along with the data, without adding additional overhead.

It was considered to add a signature to the fragment messages in data sessions, but as fragments can be re-transmitted out of order and errors can also affect the number of fragments used in following transmissions, it has an impact on mapping the signature to specific fragments. A further benefit of using the proposed Signed Segment Header is that short messages can also be authenticated.

Further discussion may be needed to update the segment diagrams in [1].

Various individual messages in [2] are defined to include a dedicated fields for authentication support. If authentication is supported at the segment level, it implies that all messages defined in [2] can be authenticated if required, and these dedicated fields can be removed.

# Proposed changes

The following changes are proposed to ITU-R M.2092 and IALA Guideline G1117.

## ITU-R M.2092

1. Proposed changes to ITU-R M.2092

| **Comment Number:**  **Name-#** | **Annex / Section** | **Section, Table, Figure** | **Type of change** | **Reason for the change, or what you want to accomplish** | **Proposed change to ITU-R M.2092-1** |
| --- | --- | --- | --- | --- | --- |
| SP-1 | 4 | 4.15 | Tech. | Introduction of Fingerprint to find digital certificate for a signature. | See below |
| SP-2 | 4 | Table 43 | Tech. | TBB payload addition of fingerprint | See below |
| SP-3 | 5 | Table 69 | Tech. | SBB Fragment 5: addition of fingerprint | See below |
| CML-1 | 4 | Section 4.29.1 | Tech. | Introduction of optional signed segment header, to support authentication at the VDES Link Layer. | See below |

### SP-1

**4.15 Digital signature of messages**

It is assumed that a public key infrastructure (PKI) is established with an international organization capable of acting as certificate authority (CA), and that Recommendation ITU-T X.509 (10/2016) is used for public key certificates and the PKI implementation. For VDES the primary purpose is to authenticate messages by attaching a digital signature.

It should be possible to store certificates and certificate revocation lists for the authentication of digital signatures and of new certificates in the VDES unit to refer to when a network connection is not available. Both certificate validation data storage and real-time network access to the CA are done by using the VDES unit PI. In case the verification of the signature fails on the VDES mobile station the message cannot be trusted. For Link Layer messages, such as the bulletin board, the system shall act as if it never had received the message.

Cryptographic algorithm for the end-entities digital signatures is the elliptic curve digital signature algorithm. The elliptic curve cryptography public key shall therefore be 256 bits. With this key size, the recommendations from Internet Engineering Task Force (IETF) Document [RFC 5480](https://datatracker.ietf.org/doc/rfc5480/) states that the minimum bits of security should be 128, the message digest algorithm Secure Hash Algorithm (SHA)-256, using IEEE P1363 Fixed-Field Concatenation format.

A digital certificate fingerprint, consisting of the 48 least significant bits of a certificate’s signatureValue (see RFC5280, 4.1.1.3), is used to identify the certificate that should be used to validate the signature.

[editorial note: the footnote referring to RFC5280 should stay]

### SP-2

Table 43 (*end*)

| Field No. | Value  (dec) | Size  (bytes) | Function | Content |
| --- | --- | --- | --- | --- |
| 6 |  | 9 | Control station service area | Parameter (longitude and latitude) defining the control station service area.  See Table 44 – control station service area. |
| 7 |  | 6 | Digital Certificate Fingerprint | See § 4.15, Annex 4 |
| 8 |  | 64 | Digital signature | Signature over the complete BB payload, see § 4.15 |

### SP-3

Table 69

Satellite bulletin board (Fragment 5)

|  |  |  |  |
| --- | --- | --- | --- |
| Field  No. | Size  (bytes) | Function | Content |
| 1 | 1 | Type | SBB digital signature part 1.  Type = 5. |
| 2 | 6 | Digital Certificate Fingerprint | Refer § 4.15, Annex 4 |
| 3 | 32 | Digital signature part 1 | Signature over BB fragments 1-4 and field 1-2 above, refer § 4.15, Annex 4. |

### CML-1

4.29 Segmentation of VHF data exchange payload

Data to be transmitted over VDE payload should be input to equipment via the PI by using applicable international standards. If the PI input results in need of executing multiple simultaneous transactions over VDL, the equipment should process them as described in this section.

VDE payload segments get packed inside the fragment as shown in Figure 43. Each segment denotes a part of data within a transaction. Transactions under simultaneous processing are identified by different sequential IDs included in the segment header.

A segment may be signed or unsigned as indicated by the Segment type. When calculating the digital signature, the Source MMSI and Destination MMSI are prepended to the data, but it is not transmitted as part of the segment. When receiving a signed segment, the Source MMSI and Destination MMSI should be prepended to the data when authenticating the signature.

4.29.1 Segment description

Table 54

Segment description

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Field  No. | Value  (Dec) | Size  (Bits) | Function | Content |
| 1 | 0 | 2 | Segment type | Default unsigned segment type |
| 2 | 0 to 214-1 | 14 | Sequential ID | Sequential ID of matching data transaction. |
| 3 | 0 to 216-1 | 16 | Payload size | Size of the segment payload data only (bytes). |
| 4 |  | Variable | Payload data | Payload data. |

Table 55

Signed segment description

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Field  No. | Value  (Dec) | Size  (Bits) | Function | Content |
| 1 | 1 | 2 | Segment type | Signed segment type |
| 2 | 0 to 214-1 | 14 | Sequential ID | Sequential ID of matching data transaction. |
| 3 | 0 to 216-1 | 16 | Payload size | Size of the segment payload data only (bytes). |
| 4 |  | Variable | Payload data | Payload data. |
| 5 |  | 32 | Timestamp | UTC time when this message is prepared in the VDES equipment, number of seconds since 1 January 2000, 00:00:00 UTC. |
| 6 |  | 48 | Digital certificate fingerprint | See § 4.15 |
| 7 |  | 512 | Digital signature | Digital signature calculated over the following data:   1. 32 bits of Source MMSI 2. 32 bits of Destination MMSI (Value of 0 for broadcast) 3. All the signed segment description fields above from field 1 to 6,   See § 4.15 |

## IALA guideline G1117

| **Comment Number:**  **Name-#** | **Annex / Section** | **Section, Table, Figure** | **Type of change** | **Reason for the change, or what you want to accomplish** | **Proposed change to ITU-R G1117** |
| --- | --- | --- | --- | --- | --- |
| CML-2 | Annex B | B.1. | Tech. | Introduction of methods to request and report digital certificates and CRLs. | See below |

### CML-2

ANNEX B: Examples of VDE Protocol Format Messages

B.1. VPFI 0: exchange of certificates

B.1.1. Certificate Report

This report may be used to transfer one or more X.509 public certificates that may be used for authentication. This report is either sent on request for a specific certificate, or it may be sent without a request.

When multiple certificates are reported in the chain of trust, the certificates should be ordered from highest to lowest level.

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

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

Table 7. Certificate Report

| Parameter | Number of bits | Description |
| --- | --- | --- |
| VPFI | 16 | 0 |
| Message ID | 16 | 0 |
| Number of certificates in report (n) | 8 | Number of certificates in report.  Set to 0 in response to a certificate request to indicate that:  - the requested certificate is not available or  - it is a root certificate that can not be shared. |
| Certificate fingerprint[0] | 48 | Fingerprint used to identify certificate. |
| Issuer certificate fingerprint[0] | 48 | Fingerprint of certificate that issued this certificate.  The issuer certificate must be authenticated before this certificate can be authenticated. |
| Latest CRL fingerprint[0] | 48 | Fingerprint of the latest CRL issued for certificate.  Set to 0 if no CRL issued for the certificate. |
| Certificate[0] | Variable  multiple of 8. | Certificate (version 3) encoded in DER format as referenced in ITU-T X.509.  Typically 600 – 900 bytes.  Size of certificate is defined in DER encoding. |
| … | … | … |
| Certificate fingerprint[n-1] | 48 |  |
| Issuer certificate fingerprint[n-1] | 48 |  |
| Latest CRL fingerprint[n-1] | 48 |  |
| Certificate[n-1] | Variable  multiple of 8. |  |

B.1.2. Certificate Request

Requests a certificate. The receiver of this message should respond with the requested certificate.

Table 8. Certificate Request

| Parameter | Number of bits | Description |
| --- | --- | --- |
| VPFI | 16 | 0 |
| Message ID | 16 | 1 |
| Fingerprint | 48 | Fingerprint to identify the certificate requested.  This Parameter can be left empty (zero number of bits) to indicate that receiver should respond with own public certificate that can be used to authenticate the receiver. |

B.1.3. Certificate Revocation List Report

Report to transmit a certificate revocation list (CRL). This report is either sent on request for a specific CRL, or it may be sent without a request.

An issuer certificate is associated with a CRL and its fingerprint is provided in the CRL report.

Table 9. CRL Report

| Parameter | Number of bits | Description |
| --- | --- | --- |
| VPFI | 16 | 0 |
| Message ID | 16 | 2 |
| Fingerprint of CRL | 48 | Fingerprint of the CRL. |
| Fingerprint of issuer certificate of CRL | 48 | Fingerprint to identify issuer certificate of the CRL.  Set to 0 if no CRL found for requested fingerprint. |
| CRL | Variable  multiple of 8. | CRL (version 2) encoded in DER format as referenced in ITU-T X.509.  Size of CRL field is defined in DER encoding.  Set to DER encoded NULL if no CRL is found. |

B.1.4. Certificate Revocation List Request

Requests a certificate revocation list (CRL). The receiver of this message should respond with the requested CRL.

The fingerprint of both the CRL and issuer certificate are used to uniquely identify the requested CRL.

Both fingerprints should be left empty (set to zero number of bits) to request all known CRL’s.

Table 10. CRL Request

| Parameter | Number of bits | Description |
| --- | --- | --- |
| VPFI | 16 | 0 |
| Message ID | 16 | 3 |
| Fingerprint of CRL | 48 | Fingerprint to identify the CRL requested.  This Parameter can be left empty (zero number of bits) to indicate that receiver should respond with all known CRLs. |
| Fingerprint of issuer certificate of CRL | 48 | Fingerprint to identify issuer certificate or CRL requested.  This Parameter can be left empty (zero number of bits) to indicate that receiver should respond with all known CRLs. |

# Action requested of the Committee

The Committee is requested to review the proposed inputs, discuss and align views during DTEC5 and provide feedback to the submitters for inputting to ITU at the WP5B meeting in fall 2025 at the end of the DTEC5 at the latest.

Members are asked to indicate if their country wants to support the planned submission to ITU.

1. Input document number, to be assigned by the Committee Secretary [↑](#footnote-ref-2)
2. Leave open if uncertain [↑](#footnote-ref-3)