

Technical Guide

for

Interoperability Pilot for Digital Seafarer Certificate Vaults

- Pilot date: 17 September 2026
- Location: BIMCO House, Copenhagen
- Facilitator: BIMCO

Executive summary

This guide explains how participating software providers should prepare for and take part in the interoperability pilot for digital seafarer certificate vaults.

The pilot will test whether independent platforms can exchange an artificial seafarer identity and associated electronic seafarer certificates using structured data aligned with the IMO Compendium data model for electronic seafarer certificates. The test will focus on whether the exchanged data can be exported, transferred, imported, displayed and kept linked to the correct artificial seafarer identity without loss of required data or manual reconstruction.

For the purpose of this pilot, interoperability means that a receiving platform can correctly interpret and use the certificate and identity data provided by another platform, even if the two platforms use different internal architectures, user interfaces or transport mechanisms. The pilot does not require all participants to use the same technical solution, but it does require the exchanged data to remain complete, readable and associated with the correct artificial identity after import.

The pilot is based on the current maturity of electronic maritime certificates, where many certificates are still digital versions of paper certificates and verification may rely on checking the issuer source, such as a flag State administration or training provider. The pilot therefore does not test legal reliance, equivalence between credentials, formal acceptance by authorities, or full verification. However, where such questions arise during the exchange (the pilot), they will be recorded as practical interoperability issues that may require further guidance, policy or standardisation at IMO or industry level.

The pilot is not a product comparison, procurement exercise, certification activity, compliance audit, cyber-security test or commercial assessment. Its purpose is to demonstrate whether seafarers can transfer an artificial certificate portfolio between digital certificate vault providers, for example when changing employer or assignment, without data degradation and loss of certificates.

Scope of the pilot

The pilot has five practical objectives:

1. Demonstrate that a seafarer identity can be exported from one independent platform and imported into another platform.

2. Demonstrate that electronic seafarer certificates can be exported from one independent platform and imported into another platform.
3. Verify that the imported certificates remain associated with the correct seafarer identity.
4. Verify that required data fields are preserved, readable and usable after exchange.
5. Identify implementation issues that may need further harmonisation, guidance or clarification.

A successful pilot does not require all participating platforms to implement the same internal architecture, user interface or transport mechanism. It requires that the exchanged identity and certificate data can be correctly understood, imported, displayed and associated by another platform using the agreed reference model and exchange approach.

Participants are not expected to disclose source code, proprietary algorithms, detailed system architecture, production credentials, private keys or commercially sensitive implementation details. The purpose is to demonstrate practical data exchange and portability, not to assess or compare individual commercial solutions.

All data used during the pilot shall be artificial or fictitious. No real personal data shall be used, displayed, exchanged or retained as part of the pilot.

The interoperability pilot will be conducted under the Chatham House Rule, meaning that information shared during the exercise may be used, but neither the identity nor the affiliation of participants will be disclosed.

BIMCO will facilitate the pilot and may record high-level observations, validation results and general lessons learned. BIMCO will not publish individual participant rankings, provider-specific pass/fail results or commercial assessments, unless otherwise decided by the participants. Any reporting from the pilot will focus on the overall interoperability concept, common technical observations and possible areas for further harmonisation.

Participation requirements

Participation is limited to digital certificate vault solution providers actively taking part in the interoperability exercise.

To maintain a practical and collaborative technical environment:

- Each participating company shall be represented by technical personnel able to operate the platform during the pilot.
- Each platform shall act both as a sending platform and as a receiving platform.
- Participants shall share sufficient technical details of their proposed exchange approach with BIMCO and the other participating providers in advance of the pilot. This could include, e.g. the intended transport mechanism, payload format, authentication or consent flow, sample payloads using artificial data, and any endpoint, sandbox or file-exchange instructions needed to perform meaningful tests.
- All test data shall be artificial or fictitious. Real seafarer personal data shall not be used.
- The pilot shall be conducted in a positive, collaborative and non-competitive manner.
- BIMCO will facilitate the exercise and record neutral observations but will not rank, score, endorse or certify individual solutions.

We hope that the participating companies will remain technical, collaborative and focused on interoperability – and perform the discussions in a good spirit.

Technical assumptions and constraints

The following assumptions apply unless otherwise confirmed by BIMCO before the pilot:

Topic	Assumption for the pilot
Reference model	The exchanged data shall be aligned with the IMO Compendium reference data model for electronic seafarer certificates, to the extent implemented by the participant. Link to IMO Compendium, 2026 version FAL.5/Circ. 56: https://imocompendium.imo.org/public/IMO-Compendium/Current/index.htm
Transport mechanism	The pilot does not prescribe a single transport mechanism. Participants shall state which mechanism they intend to use, such as structured file exchange, API exchange, sandbox-to-sandbox exchange or secure upload/download. Sufficient technical details and transport mechanisms shall be shared in advance of the pilot to allow meaningful tests to be planned and executed.
Payload format	Participants shall state the format they intend to exchange, such as JSON, XML or another structured format.
Identity matching	The receiving platform shall be able to associate imported certificates with the correct imported artificial identity following the payload format.
Manual intervention	Manual configuration may be recorded, but manual reconstruction or re-entry of certificate data should not be required for a successful exchange.
Evidence	BIMCO may record high-level observations and validation results. Any retention of screenshots, logs or exchanged files shall follow the confidentiality arrangements agreed for the pilot. Evidence may also include whether the receiver could access, interpret or preserve issuer-source verification references and any status or authentication data included in the exchange package.
Verification model	The pilot is based on the current electronic certificate model in which verification may rely on checking the issuer source, such as a flag State administration, recognised organisation or training provider. The pilot does not require all exchanged credentials to be verifiable credentials, nor does it require certificate verification to be performed as part of the exchange process.
Verifiable credentials and digital identifiers	Where participants support verifiable credentials, decentralised identifiers or other digital identifier models, this may be described as an implementation feature. Such support is not required for participation. Observations may be recorded to inform future IMO considerations or standardisation work.
Technical coordination before pilot	Participants should provide sufficient information about endpoints, API methods, authentication or consent processes, test credentials, file structures, schemas and sample artificial payloads before the pilot so that sender-receiver test pairs can be prepared.

Preparation required from each participant

Each participant shall complete the following preparation before arriving at the pilot.

Prepare an artificial seafarer identity

Each participating solution provider shall first create one artificial seafarer identity in its own platform. This may have been created in advance.

The identity shall be treated as a test profile only and shall not represent, refer to or identify a real person. All associated identity data, including name, date of birth, nationality, unique identity reference and photo, shall be fictitious or artificially generated.

After the artificial seafarer identity has been created, the platform shall issue a Seafarer Identity and Record Book (SIRB), or an equivalent digital identity record (a Seaman's Book, Continuous Discharge Certificate (CDC), or Seagoing Service Record Book), for that test identity.

The SIRB or equivalent record should be structured in accordance with the ILO Convention No. 185 Seafarer's Identity Document data structure, to the extent supported by the platform. The issued identity record shall serve as the identity anchor for the pilot and shall be used to link the two electronic seafarer certificates prepared for later tests.

The SIRB may contain the following data points:

Data element	Requirement	IMO data point
Type of certificate	Required	IMO1008
Seafarer's surname	Required	IMO0098
Seafarer's middle name	Optional	Part of IMO0100
Seafarer's given name	Required	IMO0100
Seafarer's gender	Required	IMO0099
Date of birth	Required	IMO0097
Place of birth	Recommended	IMO0106
Seafarer's nationality	Required	IMO0105
Seafarers' unique identity reference	Required	IMO0965
Photo of seafarer	Required	IMO0964
Seafarer's digital signature	Required	IMO0963
Seafarer's book number	Required	IMO0968
Issue date	Required	IMO0966
Renewal date	Required	IMO0967
Name of issuing authority	Required	IMO1023
Digital reference for authentication	Recommended	IMO1025
Logo of the issuing entity	Required	IMO1083

Electronic certificates

Each participant shall additionally prepare two electronic certificates linked to the artificial seafarer identity. The certificate types may be chosen by the participant.

Examples of suitable certificate types include Certificate of Competency, Certificate of Proficiency, STCW endorsement, Basic Safety Training certificate, Advanced Fire Fighting certificate, GMDSS certificate, Medical Certificate, Security Awareness certificate or tanker-related endorsement.

Each of the two certificates shall

- be structured according to the IMO Compendium data model for electronic seafarer certificates, to the extent implemented by the participant.
- contain realistic but fictitious certificate data.
- be exportable from the participant platform.
- be capable of being imported by another platform, subject to the agreed exchange method.
- remain associated with the artificial seafarer identity after the exchange.

Before the pilot, each participating company shall provide BIMCO with a short description of the two electronic certificates it intends to use for the exchange test. The information should be provided according to the table below and should identify the relevant data elements, whether they are required or optional, and the corresponding IMO Compendium data points where applicable.

Template for the table to be filled in prior to the test.

Data element	Requirement	IMO data point
Type of certificate	Required	IMO1008
Seafarer's surname	Required	IMO0098
...	...	...
Issue date	Required	IMO0966
Renewal date	Required	IMO0967
Name of issuing authority	Required	IMO1023
...	...	...

Provide a pre-pilot technical declaration

Each participant should return the following information to BIMCO before the pilot.

Item	Participant response
Company name	
Platform name	
Technical contact name and email	
Technical representatives attending in the pilot	
IMO Compendium version or reference implemented	
Certificate types prepared for the pilot	
Identity export supported by the platform	Yes / No / Partial
Identity import supported by the platform	Yes / No / Partial
Certificate export supported by the platform	Yes / No / Partial
Certificate import supported by the platform	Yes / No / Partial
Supported payload formats	JSON / XML / API payload / other
Exchange mechanism proposed for pilot	File exchange / API / sandbox / secure upload-download / other
Authentication method, if relevant	
Artificial identity prepared	Yes / No
Seafarer's Identity Document prepared	Yes / No
Two certificates prepared	Yes / No
No real personal data used	Confirmed / Not confirmed
Known limitations or assumptions to be shared prior to the pilot	
Detailed transport mechanism and flow shared with BIMCO	Yes / No / Partial
API endpoint, sandbox, or file-exchange instructions provided, if relevant	
Authentication, consent or user-authorisation flow described	
Issuer-source verification reference or method included, where available	
Credential status or revocation information included, where available	
Use of verifiable credentials or digital identifiers, if supported	Yes / No / Not applicable
Sample artificial payloads shared before pilot	Yes / No

This example is illustrative only and does not prescribe a mandatory transport mechanism. The important requirement is that the selected mechanism can be understood, tested and evidenced by both sending and receiving platforms using artificial data.

Where API exchange is proposed, the participant should describe the request flow at a level sufficient for another platform to test against it. For example, an API-based flow may allow a requesting platform to identify the data it wishes to receive, trigger an email to the authenticated user repeating the requested information and providing a code, retain a token returned in the initial API response, and then submit the code and token in a second request. If the code and token match, the sending platform may respond with the relevant certificate and identity data in JSON, or another agreed structured format.

To support meaningful tests, BIMCO should collect and circulate a concise technical interface pack from each participant before the pilot. The pack should contain the proposed transport mechanism, payload format, schema or field mapping, authentication or consent flow, sample artificial payloads, and any sandbox, endpoint or file-exchange instructions needed by the receiving platform.

Pre-pilot technical coordination

Exchange package to be prepared

For each exchange, the sending platform should make available an exchange package containing the artificial identity, the SIRB, and the two associated certificates. The exact packaging may depend on the participant's technical implementation and the agreed exchange method, but the receiving platform should be able to identify the identity record, the certificate records and the relationship between them.

Package element	Purpose	Expected treatment by receiver
Identity record	Provides the artificial seafarer identity to which certificates are attached.	Import or create the corresponding identity record.
SIRB record	Provides the seafarer's identity.	Import and link to the correct identity.
Certificate record 1	Provides the first electronic seafarer certificate.	Import and link to the correct identity.
Certificate record 2	Provides the second electronic seafarer certificate.	Import and link to the correct identity.
Relationship reference	Shows which identity is the holder of each certificate.	Preserve the link between identity and certificate.
Metadata / validation information	Describes format, schema version, issue status or verification reference where available.	Use for validation and record any unsupported fields.
Issuer-source verification reference	Identifies the issuer source or verification location, where available.	Preserve the reference and record whether it can be displayed or used for verification.
Credential status or validity information	Indicates current validity, revocation or status information, where supported.	Preserve the status information and record whether it can be interpreted.
Authentication or consent artefact	Describes token, code, user-consent or other exchange artefact used by the selected transport mechanism, where relevant.	Use only for the pilot exchange and do not retain beyond the agreed confidentiality arrangements.

Participants are encouraged to bring concise technical material that helps explain and execute the exchange. The following may be useful:

Where the participant intends to use an API or sandbox-based flow, the material should be shared in advance rather than only being brought to the pilot. This should include enough detail for the receiving platform to prepare a test client or equivalent test process using artificial data.

- Short platform description and scope of implementation.
- High-level description of import/export flow.
- Supported payload formats and schemas - were available.
- API documentation or OpenAPI/Swagger file, where relevant.
- Sample payloads using artificial data.
- Validation rules or known constraints.
- Sandbox access instructions, if a sandbox is used.
- Known limitations or unsupported fields.
- High-level security and authentication description - were relevant.

Participants are not required to disclose source code, proprietary algorithms, detailed internal architecture, production credentials, private keys or commercially sensitive material.

Pilot test sequence

The pilot will be conducted as a structured sequence of test steps. Each participant shall act both as a sending platform and as a receiving platform.

Before the on-site test sequence, BIMCO should confirm that each participant has shared its technical interface pack and that the relevant sender-receiver pairs understand the selected transport mechanism, payload format and authentication or consent flow.

Step 1: Readiness check

Each participant confirms that the artificial identity has been created, the SIRB and the two certificates have been prepared, export functionality is available, import functionality is available, the technical representative can operate the platform, and no real personal data is used.

Step 2: Export identity

The sending participant selects the artificial seafarer identity and exports or transfers the identity data using the agreed exchange method. The sending participant confirms which identity fields are included.

Where the agreed exchange method includes an API, token, code, authenticated email or equivalent user-authorisation step, this flow should be demonstrated using the artificial identity and recorded as part of the technical observations.

Step 3: Import identity

The receiving participant receives the identity data, imports it into its platform, creates or updates the corresponding identity record, and displays the imported identity. The sender and receiver compare the original and imported identity data.

Step 4: Export certificates

The sending participant selects the SIRB and the two prepared certificates linked to the artificial identity and exports or transfers the certificate data. The sending participant confirms which certificates and data fields are included.

Step 5: Import certificates

The receiving participant imports the certificates, links them to the correct artificial identity, displays the imported certificates, and confirms whether all required data fields remain present and readable.

Step 6: Portfolio reconstruction

The receiving platform demonstrates that the artificial identity and certificates form a coherent seafarer certificate portfolio. The portfolio shall be readable without manual reconstruction of certificate data.

Step 7: Multi-platform exchange

Each participant sends data to, and receives data from, one or more other participating providers according to the exchange matrix issued for the pilot by BIMCO.

Step 8: Data integrity verification

The sending and receiving participants jointly verify whether the key identity and certificate data fields have been preserved. Any missing, changed, manually corrected or unsupported fields are recorded.

Step 9: Issue and limitation recording

Any issues are recorded in a neutral manner. Issues may relate to data model interpretation, field mapping, exchange format, transport mechanism, validation rules, identity matching, certificate linking or unsupported fields.

Step 10: record practical interoperability issues

Issues should also be recorded where they relate to reliance, equivalence, issuer-source verification, credential status, authentication flow, user consent, or the ability of the receiving platform to preserve verification references. These observations should be framed as common learning points rather than provider-specific assessments.

Success criteria

The pilot seeks to demonstrate that:

- An artificial seafarer identity can be exchanged between independent platforms.
- Electronic seafarer certificates can be exchanged between independent platforms.
- Imported certificates remain linked to the correct artificial identity.
- Required identity and certificate data remains complete and readable.
- No certificate is lost during the exchange.
- No certificate requires manual reconstruction after import.
- A seafarer certificate portfolio can be reconstructed on another platform.
- Participants can both send and receive certificate data.
- Observed issues can be described in a way that supports future harmonisation and improvement.

Evidence and confidentiality

The pilot requires enough evidence to support a credible neutral summary of the exercise, while protecting confidential and commercially sensitive information. Participants should be prepared to allow BIMCO to record validation outcomes and high-level observations. Any retention of screenshots, logs, payloads or sample files shall be handled according to the confidentiality arrangements agreed for the pilot.

- BIMCO will not publish comparative rankings or provider-specific pass/fail results.
- BIMCO will not disclose commercially sensitive implementation details without prior agreement.
- Issue descriptions should focus on technical cause and learning point rather than provider performance.

- Where observations concern reliance, equivalence, verification or future use of verifiable credentials, they should be recorded as potential topics for further IMO or industry guidance rather than as deficiencies in individual systems.
- No real personal data shall be submitted, displayed or retained as part of the pilot.

BIMCO will publish a high-level summary of the pilot (workshop) outcomes, focusing on interoperability concepts and lessons learned, without identifying or evaluating individual providers. The report is intended for submission to the IMO Facilitation Committee (FAL 51) in Spring 2027 and will be circulated to participants for review and approval before submission.

We hope that the participating companies will remain technical, collaborative and focused on interoperability – and perform the pilot and discussions in a good spirit.

Any questions concerning the pilot or workshop should be directed to:

Jeppe Skovbakke Juhl

Chief Naval Architect

BIMCO

Email – jsj@bimco.org

/BIMCO, July 2026

Annex A

Sample structure for artificial identity and certificates

The example below is not a mandatory schema. It illustrates the type of structured information that could be included in an exchange package. Participants should adapt the structure to the agreed IMO Compendium mapping and their own implementation.

IMO_DATASET_COMPENDIUM_V1.json

```
const SeafarerRecordBook = {  
  "TypeofCertificate": "IMO1008",  
  // Core Identification  
  "Person flag State ID identifier [BMA SEAFARER ID]": "IMO0971",  
  "SURNAME/ FAMILY NAME": "IMO0098",  
  "GIVENNAME": "IMO0100",  
  "DATE OF BIRTH": "IMO0097",  
  "NATIONALITY": "IMO0105",  
  //Certificate Data  
  "Seafarer Record Book number": "IMO0968",  
  "The name of the issuing entity": "IMO1023",  
  //Verification Status  
  "Person Seafarer Record Book issue date": "IMO0969",  
  "Person Seafarer Record Book expiry date": "IMO0970",  
  "valid_until": "IMO0970",  
  "status": "IMO1011",      //"VERIFIED"  
  "ledger_hash": "IMO1025", //"0x7f...3a2"  
};
```

Annex B

Participant readiness checklist

Checklist item	Confirmed	Comment
Artificial seafarer identity created		
Seafarer's Identity & Record Book created		
Two electronic certificates created		
Certificates linked to artificial identity		
No real personal data used		
Export method tested internally		
Import method tested internally		
Payload format identified		
Exchange method identified		
Technical representative attending		
Known limitations shared with BIMCO		
Technical interface pack shared with BIMCO		
Transport mechanism and flow described		
Authentication or consent flow described, if relevant		
Sample artificial payloads shared		
Issuer-source verification reference included, where available		
Credential status information included, where available		

Annex C

Validation sheet for each exchange

Validation point	Result	Comment
Identity received and imported	Pass / Partial / Not completed	
Identity key fields preserved	Pass / Partial / Not completed	
Photo or photo reference preserved, where supported	Pass / Partial / Not completed	
SIRB received and imported	Pass / Partial / Not completed	
Certificate 1 received and imported	Pass / Partial / Not completed	
Certificate 2 received and imported	Pass / Partial / Not completed	
Certificates linked to correct identity	Pass / Partial / Not completed	
Required certificate fields preserved	Pass / Partial / Not completed	
No manual reconstruction of certificate data required	Pass / Partial / Not completed	
Issues recorded if any	Yes / No / Not applicable	
Transport mechanism executed as described	Pass / Partial / Not completed	
Authentication or consent flow completed, where relevant	Pass / Partial / Not completed	
Issuer-source verification reference preserved, where available	Pass / Partial / Not completed	
Credential status information preserved, where available	Pass / Partial / Not completed	
Practical interoperability issue recorded, if any	Pass / Partial / Not completed	

