

ICS 35.240.60; 47.020.99

Smarte Logbücher für die Schifffahrt; Text Englisch

Smart logbooks for shipping;
Text in English

Les journaux intelligents pour la navigation;
Texte en anglais

Zur Erstellung einer DIN SPEC können verschiedene Verfahrensweisen herangezogen werden:
Das vorliegende Dokument wurde nach den Verfahrensregeln einer PAS erstellt.

Gesamtumfang 60 Seiten

Contents

	Page
Foreword	5
Introduction.....	6
1 Scope	7
2 Normative references	7
3 Terms and definitions.....	7
4 Symbols and abbreviations.....	8
5 Requirements.....	9
5.1 Units.....	9
5.2 Power supply.....	9
5.3 Minimum requirements for smart components (offline functionality)	9
5.4 Authentication and digital signatures	10
5.5 Installation and user instructions	10
5.6 Display	10
5.7 Interface.....	11
5.7.1 Input interfacing	11
5.8 Data handling.....	12
5.9 Functions	13
5.9.1 Calculations.....	13
5.9.2 Analysis	13
5.9.3 Notifications	13
5.9.4 Filter	13
5.9.5 Export.....	13
5.10 Alerts and Failures	13
5.10.1 Alert management.....	13
5.10.2 Backup and fall-back arrangements.....	14
5.11 Security (updates)	14
5.12 Equipment familiarisation and documentation.....	15
5.12.1 General	15
5.12.2 Operating manuals.....	15
5.12.3 Installation manuals.....	15
5.12.4 On-board familiarisation material.....	16
6 Test methods.....	16
6.1 Units.....	16
6.2 Power supply.....	16
6.3 Minimum requirements for smart components (offline functionality)	16
6.4 Authentication and digital signatures	16
6.4.1 General	16
6.4.2 Import of public/private key pairs	17
6.4.3 Generation of public/private key pairs.....	17
6.4.4 Import of X.509 certificates	17
6.4.5 Other means	18
6.5 Installation and user instructions	18
6.6 Display	18
6.7 Interface.....	18
6.7.1 Input interfaces	18

6.7.2	VDR interface	19
6.7.3	Alert management interface.....	19
6.7.4	System and status interface	19
6.8	Data handling.....	19
6.9	Functions	20
6.9.1	Calculations	20
6.9.2	Analysis	20
6.9.3	Notifications	20
6.9.4	Filter.....	20
6.9.5	Export	20
6.10	Alerts and Failure.....	20
6.10.1	Alert Management.....	20
6.10.2	Backup and fall-back arrangements.....	21
6.11	Security (updates).....	21
6.12	Equipment familiarisation and documentation.....	21
Annex A	(normative) Logbook data exchange formats	22
A.1	General.....	22
A.2	XML-based exchange format	23
A.2.1	Document element.....	23
A.2.2	Record element	27
A.2.3	Amendment element.....	28
A.2.4	Approval element.....	29
A.2.5	Extension element.....	31
A.2.6	XSD Schema of the logbook exchange format	31
A.3	JSON-based exchange format	51
A.3.1	Document objects.....	52
A.3.2	Record objects	54
A.3.3	Entry objects.....	55
A.3.4	Amendment objects.....	56
A.3.5	Approval objects.....	57
A.3.6	Extension objects.....	58
A.3.7	Digital signature	58
Bibliography		60

Tables

Table A.1	— Content of Document element	24
Table A.2	— Attributes of Document element.....	25
Table A.3	— Vessel and voyage details of Document element.....	25
Table A.4	— Content of Record element	27
Table A.5	— Content of Entry element.....	27
Table A.6	— Content of Amendment element.....	28
Table A.7	— Content of Delete element.....	29
Table A.8	— Content of Replaced element	29
Table A.9	— Content of Approval element	29
Table A.10	— Content of reference elements.....	30
Table A.11	— Content of Extension element	31
Table A.12	— Properties of Document object.....	52

Table A.13 — Optional properties of Document object.....52

Table A.14 — Properties of Record object 54

Table A.15 — Properties of Entry object.....55

Table A.16 — Properties of Amendment object.....56

Table A.17 — Properties of Approval object 57

Table A.18 — Properties of reference object 57

Table A.19 — Properties of Extension object.....58

Table A.20 — Properties of SignInfo object.....58

Table A.21 — Properties of KeyInfo object.....59

Foreword

This DIN SPEC has been developed according to the PAS procedure. The development of a DIN SPEC according to the PAS procedure is carried out in DIN SPEC (PAS)-consortiums and does not require the participation of all stakeholders.

This document has been developed and adopted by the initiator(s) and authors named below:

- NautilusLog GmbH
Otto Klemke
- Raytheon Anschütz GmbH
Gunar Fiedler
- Korean Register KR Hamburg GmbH
Michael Suhr
- Marsig GmbH
Kathleen Kuhn

At present, there are no standards covering this topic in the body of German Standards.

DIN SPEC (PAS)s are not part of the body of German Standards.

A draft of this DIN SPEC (PAS) has not been published.

Despite great efforts to ensure the accuracy, reliability and precision of technical and non-technical information, the DIN SPEC (PAS)-consortium cannot give any explicit or implicit assurance or warranty in respect of the accuracy of the document. Users of this document are hereby made aware that the consortium cannot be held liable for any damage or loss. The application of this DIN SPEC (PAS) does not release users from the responsibility for their own actions and is applied at their own risk.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. DIN shall not be held responsible for identifying any or all such patent rights.

Provision of this document free of charge as a PDF via the Beuth WebShop has been financed in advance.

Introduction

Enhancing the ISO 21745, Electronic record books for ships — Technical specifications and operational requirements, this document describes smart technologies for electronic logbooks which simplify and automate the documentation and also increase data quality and security.

Increasing competitive pressure in the maritime industry, new regulations, the need for optimisation and autonomous ships will require more useable data in the future.

1 Scope

This DIN SPEC applies to operational and performance requirements for smart logbooks. It is applicable for documentation, process management, connection and data collection through person (human-machine-interface/smartphone), IOT/ sensors and third-party systems.

It defines a complement to ISO 21745 "Electronic record books for ships — Technical specifications and operational requirements".

NOTE Smart logbooks are mobile solutions based on smartphones or IoT which make it possible to collect confidentially data directly on board, evaluate it and control procedures.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

DIN EN 61162 (all parts), *Maritime navigation and radiocommunication equipment and systems — Digital interfaces*

DIN EN 61996-1, *Maritime navigation and radiocommunication equipment and systems — Shipborne voyage data recorder (VDR) — Part 1: Performance requirements, methods of testing and required test results*

DIN EN 62288:2015-05, *Maritime navigation and radiocommunication equipment and systems — Presentation of navigation-related information on shipborne navigational displays — General requirements, methods of testing and required test results (IEC 62288:2014); English version EN 62288:2014*

DIN EN 82079-1, *Preparation of instructions for use — Structuring, content and presentation — Part 1: General principles and detailed requirements*

DIN EN IEC 61162-450, *Maritime navigation and radiocommunication equipment and systems – Digital Interfaces — Part 450: Multiple talkers and multiple listeners – Ethernet interconnection*

DIN EN IEC 62923 (all parts), *Maritime navigation and radiocommunication equipment and systems — Bridge alert management*

DIN ISO 8601, *Data elements and interchange formats — Information interchange — Representation of dates and times*

ISO 639-3, *Codes for the representation of names of languages — Part 3: Alpha-3-Code for comprehensive coverage of languages*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <http://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

DIN and DKE maintain terminological databases for use in standardization at the following addresses:

- DIN-TERMinologieportal: available at <https://www.din.de/go/din-term>
- DKE-IEV: available at <http://www.dke.de/DKE-IEV>

3.1

mobile device

non-stationary device that can be moved around

EXAMPLE Smartphones, tablets.

3.2

data core unit

device with high availability and reliability to implement the core functions of a smart logbook

Note 1 to entry: The data core unit is a part of the smart logbook.

Note 2 to entry: The data core unit has privileged data access and higher responsibilities regarding data persistence, consistency.

3.3

data collection unit

I/O unit

optional and additional input/output device providing distributed access to data of the logbook and support for input and collection of logbook records from various sources being it manual input or automatic collection via sensors of any kind

Note 1 to entry: It is part of the smart logbook.

3.4

master user

user of the smart logbook with a privileged role such as "master" or of similar regulatory importance to the logbook content

3.5

operator

any user of the smart logbook that is not a master user including users that are only allowed to read data or that can supply data inputs that not directly become part of the legally binding logbook content

3.6

gateway

unit acting as data exchange interface between the logbook units and the vessel's onboard systems (i.e. bridge, sensors network)

3.7

critical software bug

error or problem in the software run on the smart logbook unit that could potentially lead to inconsistent data, software crashes or other software behaviour violating the mandated functionality described

3.8

critical software update

update of the software containing fixes for at least one critical software bug

4 Symbols and abbreviations

BAM Bridge Alert Management

CA Certification Authority

CAM Central Alert Management

CCRP Consistent Common Reference Point

EUT Equipment under test

HBT	Heartbeat (defined in DIN EN 61162-1)
INS	Integrated Navigation System
IoT	Internet of Things
LED	Light-emitting diode
NTP	Network Time Protocol
SD-card	Secure digital memory card
UDP	User datagram protocol
USB	Universal serial bus
UTC	Coordinated universal time
VDR	Voyage Data Recorder

5 Requirements

5.1 Units

The smart logbook shall consist of at least two data core units.

Additional core units and/or I/O units can be added to the smart logbook to expand functionality.

5.2 Power supply

Data core units shall be connected to a permanent power supply (main power supply).

Data core units shall be equipped with a backup power supply to compensate power outage from the main power supply for at least four hours for one core device. The manufacturer shall provide guidance to the user to ensure that the backup power supply meets the requirement. Options for backup power supply include:

- external or internal batteries, potentially charged from main power supply;
- secondary permanent power supply not dependent on the main power supply.

Data core units shall automatically switch to backup power supply in case of an outage of main power supply and shall automatically switch back to main power supply after the outage has been resolved. Data core and data collection units may display an indication to notify that they run on backup power supply in case of missing main power supply.

Switching the power supply of any unit shall not damage previously persisted data or lead to corruption of data currently recorded while the outage occurs and the power supply is switched.

5.3 Minimum requirements for smart components (offline functionality)

Data collection units shall provide their assigned functionality also in the case that no connection to data core units is available.

Data recorded by any unit shall initially be stored directly on the unit that recorded the data. Breaking or missing connectivity to other units shall not lead to inconsistent data recording.

Units shall notify the user if they have not contacted the network of other units (if any) or have not synchronized their data for at least 4 h to 8 h. These notifications shall be repeated at least every 10 min until synchronisation is finished successfully. During synchronization the notifications may be suppressed. Units shall inform the user either visually (e.g. devices with display) and/or by other suitable methods (e.g. haptic feedback or audible indications).

5.4 Authentication and digital signatures

The equipment shall use digital signatures to authenticate the source of logbook data and to provide means for checking the integrity of logbook data.

The equipment shall provide at least one of the following means for maintaining the infrastructure for digital signatures for each user account of the equipment:

- 1) import or generation of public/private key pairs; or
- 2) import of X.509 certificates signed by a trusted root CA; or
- 3) other means (such as hardware security modules) which are suitable to authenticate the user and digitally sign the logbook data.

The manufacturer shall describe the provided means in the installation manuals, including the algorithms used for digital signatures of logbook data.

The equipment shall provide means to revoke private keys or certificates which cannot be trusted anymore.

Import, generation, and revocation of keys and certificates shall be recorded in the equipment's audit log.

To allow stakeholders to verify the integrity of the logbook data, the equipment shall provide means to export the public keys of all users to an external storage medium. Alternatively, means shall be described in the operating manuals how to obtain the public keys of the users, e.g. from a public directory.

The equipment shall sign all recorded logbook data using the private key of the user which generated the data. If data is automatically recorded independently from a user, the data shall be signed using a private key of the equipment.

The digital signature algorithm employed shall make use of asymmetric cryptography and shall have equivalent security strength of at least 128 bits.

Hash functions such as MD4, MD5, and SHA-1 are considered to be insecure and shall not be used for new digital signatures. Refer to ISO/IEC 10118-3 for guidance on suitable hash functions.

5.5 Installation and user instructions

The manufacturer shall provide evidence in the installation manual that a system check shall be performed every time when changing the system set-up before it is taken into operation.

The test shall be performed automatically as far as possible, remaining items shall be checked manually.

The results shall be logged and may be displayed.

The manufacturer shall provide further instruction in the installation manual. The manufacturer shall provide in the installation manuals instructions on the equipment's location, e.g. to respect the requirements of DIN EN 60945 regarding the use of wireless networks.

5.6 Display

The displays at least of the core units shall be in accordance with the following clauses of DIN EN 62288:2015-05

- 4.3.1 Consistency of layout;
- 4.3.2 Consistent presentation of information;
- 4.4.2 Legibility of alphanumeric data and text;
- 4.4.3 Presentation of text;

- 4.4.4 Icons;
- 4.5 Colours and intensity;
- 4.6.1 Operational information;
- 4.7 Colour coding of information;
- 4.8 Integrity marking;
- 4.9.1 Operational status;
- 4.11 User manuals, instructions and reference guides.

It shall be possible to adjust the brightness of the display, as applicable to the display technology. It shall be possible to dim the display. The range of control shall permit the display to be legible under all ambient light conditions likely to be experienced on the bridge of a ship (e.g. day, dusk and night).

5.7 Interface

5.7.1 Input interfacing

The equipment shall be capable of receiving at least the ship's position, heading, course and speed from connected sensors or systems which are in accordance with recognised international standards.

The equipment shall provide DIN EN 61162 compliant interfaces to relevant sensors. The manufacturer shall declare in the installation manuals which DIN EN 61162 sentences are supported and how the data from these sentences is used for the logbook.

The equipment may use proprietary communication in addition to the DIN EN 61162 interfaces.

The equipment shall not use data from connected sensors or systems, which is marked as invalid.

As far as practical, the equipment shall check the plausibility of received data, especially the value range. The equipment shall not use data that is considered to be implausible. The manufacturer shall declare in the operating manuals which plausibility checks are performed.

As far as practical, the equipment shall check the integrity of received data. The equipment shall support at least one of the following methods for the ship's position, heading, course, and speed:

- 1) comparing the value with a value of the same kind from a second, independent source;
- 2) a model-based test such as a dead reckoning calculation; or
- 3) other suitable methods;
- 4) manual approval of the data.

The manufacturer shall declare in the operating manuals which methods for checking the integrity of data are provided.

The equipment shall mark received data, which did not pass the integrity check.

If the equipment is part of an INS or connected to an INS, it may transfer the responsibility of checking plausibility and integrity of received data to the INS. The installation manuals shall contain guidance on how to configure the equipment in this case.

The equipment shall provide an interface to a timeserver to synchronize itself to UTC time.

The interface may be based on the ZDA sentence synchronizing the time of the equipment with a GPS receiver or other protocols such as NTP.

5.7.2 VDR interface

The equipment shall provide a binary file transfer interface according to DIN EN IEC 61162-450 to the VDR for transmitting logbook data at the VDR.

The equipment shall transmit logbook data as XML or JSON files as specified in Annex A.

The logbook data (either in XML or JSON format) shall be sent as a data block according to DIN EN IEC 61162-450, re-transmittable transfer ("RrUDP"), where the "DataType" shall be set to "application/xml" for XML-formatted logbook data or "application/json" for JSON-formatted data.

The "status and information text" field in the binary file descriptor, as defined in DIN EN IEC 61162-450, shall be filled with the information required by the VDR as specified for "LAN image protocol" in DIN EN 61996-1. The "Source" class shall be set to "Logbook", optionally followed by an instance identifier separated by a dot.

NOTE Examples of transmitted sources are "Source:Logbook" or "Source:Logbook.1".

Transmissions to the VDR shall by default be addressed to the UDP multicast group 239.192.0.26, port 60026. The equipment shall provide means such that the system integrator is able to configure the multicast group and port to other appropriate values.

5.8 Data handling

All data records collected from the logbook units shall be annotated with at least the following meta data:

- an identifier representing the unit (or logical peer in the device network);
- unit's currently authenticated user (if applicable);
- point of time of data recording in UTC.

The equipment shall provide means to protect recorded data from unauthorized user access. If the raw data storage can be accessed outside of the device/software without any tools (e.g. SD cards or other removable storage devices) or the equipment is used in an unsecure environment, the equipment shall provide means to encrypt the data in a way that prevents the data from being easily read without authorization. The use of encryption shall be selectable at setting to work of the equipment.

The manufacturer shall give guidance in the installation manuals that losing the authentication credentials such as the password for unlocking the equipment may cause the loss of logbook data which is required by regulations. Recorded data shall be stored in a way such that the equipment can detect modifications, deletions, or other corruptions of data, e.g. by using digital signatures and checksums. The manufacturer shall declare in the installation manuals which means are provided.

The equipment shall provide means to export logbook data in one of the data formats specified in Annex A.

5.9 Functions

5.9.1 Calculations

The equipment shall provide means to calculate dependent data from already recorded data such as travelled distance, set and drift, true wind, etc. The manufacturer shall declare in the operating manuals which calculations are supported by the equipment.

5.9.2 Analysis

The equipment shall, as far as reasonable, analyse the recorded data and automatically detect events such as passing an aid to navigation, change of the navigational status, etc. Relevant detected events shall be recorded after confirmation by the user. The manufacturer shall declare in the operating manuals, which events are supported by the equipment.

5.9.3 Notifications

The equipment shall, as far as reasonable, provide notifications to the user when it is required to log certain data manually, e.g., hourly observations or when automatically recorded data indicate a certain event, such as begin of voyage. The manufacturer shall declare in the operating manuals, which notifications are supported by the equipment.

5.9.4 Filter

The equipment shall provide means to search for individual logbook data for example:

- 1) created within a time interval;
- 2) of a certain type;
- 3) containing certain values;
- 4) created within an geographical area.

5.9.5 Export

The equipment shall provide means to export the search result as a report to an external storage medium. The format of the report shall be designed to prevent modification and deletion of data, e.g. by providing a digital signature of the report.

5.10 Alerts and Failures

5.10.1 Alert management

The equipment shall handle, distribute, and present its alerts following the BAM concept as defined in DIN EN IEC 62923 (all parts).

The equipment shall at least fulfil all requirements for the equipment function type "P" as defined in DIN EN IEC 62923-1. If the equipment integrates components which are not BAM compliant but create alert-like information or use proprietary alert communication, it shall also fulfil the requirements for the equipment function type "S".

If the equipment provides logbook functionality in multiple clusters of the ship (e.g. deck logbook on the bridge and engine logbook in the engine room), it shall provide means to distribute alerts only to the affected clusters.

If the equipment supports multiple displays, it shall present alerts in a consistent manner on all displays which are affected by these alerts.

The equipment shall use the icons defined in DIN EN IEC 62923-1 for alert presentation.

If a display of the equipment is disconnected from the system, it shall display a permanent indication that no system and alert communication is available.

If the equipment consists of multiple devices, it shall monitor the availability of the devices and present the information to the user on request.

If the equipment consists solely of displays which can be disconnected from the equipment by the user, the equipment shall monitor the availability of displays. If no displays are available, the equipment shall report a caution on the alert management interface and it shall report its operational state as malfunctioning on the system status interface.

5.10.2 Backup and fall-back arrangements

The equipment shall be designed such that the failure of one device of the equipment does not cause the loss of:

- recording of manually entered logbook data;
- safe, secure, and durable storage of recorded logbook data.

The manufacturer shall declare the redundancy concept and fall-back arrangements of the equipment in the operating manuals.

Degraded functionality of the equipment shall be indicated to the user.

If data from connected sensors is missing, invalid, or implausible, the equipment shall provide an indication to the user that the missing data shall be manually recorded.

If the equipment provides fall-back arrangements to obtain sensor data from sources which are not in accordance with recognised international standards, this data shall be considered to be of doubtful integrity, clearly marked as such and only used after confirmation by the user.

If time synchronization to UTC is not possible, the equipment shall provide means to the user to manually synchronize the internal clock to UTC.

If no automatic position data is available, the equipment may provide a dead reckoning procedure to estimate the current position of the ship. Positions obtained from such calculations shall be marked to be of doubtful integrity and shall only be used after confirmation by the user. If a dead reckoning procedure is active, the equipment shall provide means to manually adjust the data for position, course, and speed. The operating manuals shall provide guidance on the accuracy and usability of position data obtained from dead reckoning.

If multiple instances of the equipment are operated (e.g. as part of the backup arrangements of the redundancy concept), the instances shall synchronize and merge the recorded data as far as practicable. If synchronization is not possible, data shall be stored locally on the equipment and synchronized as soon as the equipment is connected again.

5.11 Security (updates)

The unit shall display information about available software updates and problems of a currently used software version if that information is available to the unit. In case of available critical software updates or a known critical software bug in a currently used software version the unit shall display a permanent indication. This indication shall be permanently visible to the users leading to further information and instructions.

The software update procedure shall be described in the manual and shall be followed by the operator or master. The procedures shall include at least:

- declaration about the importance of software updates;
- steps to perform to update the software;
- troubleshooting instructions (e.g. failing update, possibility of roll-backs to undo last update).

Data consistency shall not be impacted by performing updates.

The interaction of units running different software versions shall not lead to inconsistent data or errors.

5.12 Equipment familiarisation and documentation

5.12.1 General

The equipment documentation shall use a clear and comprehensible language according to DIN EN 82079-1 and shall be available at least in English.

If the documentation uses or references resources on the Internet such as websites or online videos, the equipment shall ensure the availability of all required information also in the case of an unavailable Internet connection.

5.12.2 Operating manuals

Operating manuals shall include:

- 1) an overall description of the equipment's functionality;
- 2) a description how to customize the equipment;
- 3) guidance for operating the equipment including operation in a failure or fall-back situation;
- 4) a description of the redundancy concept;
- 5) a description of possible failures and their effects on the system for basic fault analysis;
- 6) a description of all alerts and indications;
- 7) limitations of the equipment, e.g. storage or data transfer capabilities or limitations imposed by unavailable interfaces to other equipment;
- 8) user guidance on cyber-security issues such as usage of USB sticks or creation of secure passwords.

The operating manual shall at least be accessible from the user interface of the equipment, e.g. as a context-sensitive help function or an electronic document. The equipment shall present the version of the operating manuals applicable for the software.

5.12.3 Installation manuals

The installation manuals shall include adequate information to allow the installation of the equipment so it can meet all requirements of this specification, including:

- 1) information on and instructions for the connection of other equipment such as sensors, VDR or CAM;
- 2) data flow schematic diagram and its interpretation;
- 3) power supply arrangements;

- 4) guidance to properly configure the CCRP and sensor positions of the vessel;
- 5) recommendations on the equipment's location and factors that may degrade performance or reliability;
- 6) guidance on troubleshooting the installation procedure;
- 7) guidance on hardware and software maintenance arrangements such as the software update procedures.

5.12.4 On-board familiarisation material

Material enabling on-board familiarisation training shall be provided for the equipment. The familiarisation material shall explain all functions, limitations, configurations, controls, displays, alerts, and indications of the equipment.

NOTE Familiarisation material shall allow a user that is generically trained but unfamiliar with the installed equipment to become rapidly acquainted with the installed system.

The equipment shall support at least one of the following methods of familiarisation:

- 1) stand-alone self-training manual; the training manual shall not be part of the general operating manuals;
- 2) training video (accessible on the equipment or on a separate medium) supported by a self-training manual;
- 3) computer-based training on the ship or remotely, e.g. from a notebook computer;
- 4) a training mode of the equipment supported by a self-training manual or by an assisted walkthrough.

6 Test methods

6.1 Units

Confirm by inspection of documented evidence that the EUT fulfills the requirements of 5.1.

6.2 Power supply

Confirm by inspection of documented evidence that the EUT fulfills the requirements of 5.2.

6.3 Minimum requirements for smart components (offline functionality)

Confirm by inspection of documented evidence that the EUT fulfills the requirements of 5.3.

6.4 Authentication and digital signatures

6.4.1 General

Confirm by observation that the EUT allows the user to export the public keys used for signing logbook data to an external storage medium.

Confirm by analytical observation that it is not possible to access or export the private keys of the user accounts at least in user mode.

Confirm by observation that automatically recorded data is signed by a system-specific private key or similar means.

Refer to the installation manuals to identify all implemented methods for authenticating the source of logbook data and checking the integrity of logbook data. Confirm by inspection of documented evidence that at least one of the following methods is provided. Confirm by analytical evaluation that the provided means use asymmetric cryptography and have equivalent security strength of at least 128 bits. Perform the following tests if the method is provided by the EUT.

6.4.2 Import of public/private key pairs

Refer to the installation manuals to identify the supported types of public/private keys. For each supported type, generate a public/private key pair by means of a third-party tool which is not part of the EUT. Import the public/private key pair into the EUT. Create a logbook record which is signed by the imported private key. Export the signed data to an external storage medium.

Confirm by observation that the signature provided in the exported data can be verified with the matching public key.

Confirm by observation that the user can revoke the private key. After revoking the private key, confirm by analytical evaluation that it is not possible to use the private key to sign logbook data.

Confirm by observation that importing the public/private key pair and the revocation of the key was recorded in the EUT's audit log.

6.4.3 Generation of public/private key pairs

Refer to the installation manuals to identify the supported types of public/private keys. For each supported type, let the EUT generate a public/private key pair.

Confirm by observation that the EUT is able to export the generated public key.

Create a logbook record which is signed by the generated private key. Export the signed data to an external storage medium.

Confirm by observation that the signature provided in the exported data can be verified with the exported public key.

Confirm by observation that the user can revoke the private key. After revoking the private key, confirm by analytical evaluation that it is not possible to use the private key to sign logbook data.

Confirm by observation that the generation of the public/private key pair and the revocation of the key was recorded in the EUT's audit log.

6.4.4 Import of X.509 certificates

Refer to the installation manuals to identify the supported types of certificates and how to obtain a certificate which can be used in the EUT. Generate a certificate.

Confirm by observation that the certificate can be imported into the EUT.

Create a logbook record which is signed by the certificate's private key. Export the signed data to an external storage medium.

Confirm by observation that the signature provided in the exported data can be verified with the public key from the certificate and that the author of the exported data is the entity for which the certificate was issued.

Generate a certificate which is not signed by a CA trusted by the EUT, e.g. a self-signed certificate.

Try to import the certificate into the EUT. Confirm by observation that the EUT rejects the import of the certificate.

Confirm by observation that the user or the CA can revoke the certificate. After revoking the certificate, confirm by analytical evaluation that it is not possible to use the certificate to sign logbook data.

Confirm by observation that importing the certificate and the revocation of the certificate was recorded in the EUT's audit log.

6.4.5 Other means

Refer to the installation manuals to identify how to sign logbook data with the provided means. Create and export a logbook record which is signed by the identified means.

Confirm by analytical evaluation that:

- the source of the logbook data (the user which entered the data) can be identified;
- the signature of the logbook data can be verified outside the EUT by tools either commonly available or provided by the manufacturer;
- the signature of the logbook data protects the data against modification and deletion;
- untrusted private keys and certificates can be revoked;
- it is not possible to use revoked keys or certificates to sign logbook data.

6.5 Installation and user instructions

Confirm by inspection of documented evidence that the EUT fulfills the requirements from 5.5.

6.6 Display

Confirm by inspection of documented evidence that the core units of the EUT fulfill the requirements of Clause 5.6.

6.7 Interface

6.7.1 Input interfaces

Connect the EUT to a simulator providing position, heading, course, and speed.

Confirm by observation that the EUT records the simulated data as "automatically collected data".

Confirm by inspection of documented evidence that the EUT provides DIN EN 61162 compliant interfaces.

Confirm by observation that the installation manuals give guidance to only connect sensors which are in accordance with recognized international standards.

For all supported input sentences, simulate invalid data as far as practicable, e.g. by setting validity flags to "V" or by invalidating checksums. Confirm by observation that the EUT does not record data which is invalid.

Refer to the operating manuals to identify the plausibility criteria supported by the EUT. Simulate data which violates these plausibility criteria. Confirm by observation that the EUT does not record data which is implausible.

Refer to the operating manuals to identify the integrity criteria supported by the EUT. Simulate data which violates these integrity criteria. Confirm by observation that the EUT marks the data to be of doubtful or failed integrity.