Kraftfahrt-
Bundesamt

Guidelines

on the reporting of manufacturers to the KBA and the Technical Service under UN-R 155/156

Revision 1.0 final, Version: 27.06.2022

Contents

Page

1 Purpose

This document explains the reporting obligations of the organisations mentioned in the scope to the KBA as a certificate granting authority and the Technical Services (TDs) operating in this context. It determines the minimum of information to be provided in the initial and renewal process and in the context of the surveillance of the certificate of conformity (CoC, further referred to as the certificate).
Form, extent and communication channel shall be agreed separately with the KBA and with the relevant TS, provided that no requirements to that are formulated in this document.
Since the TS analyses the information on behalf of the KBA, it is recommended that a reporting system based on this document is also agreed between TS and manufacturers
Information relating to granting and extension of approvals, CoP and market surveillance will only be considered in this document if it allows conclusions to be drawn on the functioning and adequacy of the management system. Other requirements for such reporting obligations not mentioned here are not affected.

2 Scope of application

This document is addressed to organisations wishing to obtain a certificate in accordance with UN Regulations 155 and 156 at the KBA, or to which such a certificate has been granted.[1]

3 Abbreviations

CSMS	Cybersecurity Management System
CVE	Common Vulnerabilities and Exposures
BSI	Federal Office for Information Security
KBA	Federal Motor Transport Office
SUMS	Software Update Management System
TS	Technical service
UN-R	UN Regulation

4 Supporting documents

Application of the Rules for designation/recognition for technical services (categories A, B, D) for testing in the context of the KBA-type approval procedure according to UN-R 155/156

5 Responsibilities

The manufacturer shall make the following information available to the KBA unsolicited.
At the request of the KBA or the competent TS, the manufacturer shall provide further information or change the frequency of the notification.
The manufacturer shall evaluate the available information regarding the effectiveness and adequacy of the management system to be monitored and shall provide the KBA and the TS correspondingly processed data in form of at least an annual report.
The TS analyses the information provided by the manufacturer and other relevant information in the context of its testing and monitoring job and provides the KBA with the result of this analysis, including proposals for decisions, if applicable.
The KBA (Dresden) evaluates the information provided by manufacturers and TS in relation to the manufacturer and the security situation and makes any necessary decisions. If the information may also be relevant for other areas of the Type Approval and Market Surveillance Divisions of the KBA, it will be forwarded accordingly. Claims made directly from other areas of the KBA or resulting from other provisions of the KBA shall remain unaffected.
An evaluation is also carried out in relation to the effectiveness and adequacy of the requirements laid down by the KBA.

[1] also referred to as the manufacturer

The BSI supports the KBA at its request. The KBA will provide the BSI with the necessary information. The KBA will also provide the BSI with information that could be essential to assess the security situation by this authority.

6 General

(1) The manufacturer shall provide the information required by the legal acts and in this guide in writing in digital editable form[2], via one of the following reporting channels to the KBA.

- E-mail: cybersecurity@kba.de
  (UN-R 155 only; PGP-based encryption is accepted)
- E-Typ
- other communication channels agreed with the KBA.

If the urgency so requires, the notification should be made in advance by telephone (telephone: 0461-316-2611).

(2) Previously established reporting channels can be maintained. In principle, the same information does not have to be reported to several addressees. However, the KBA requests to set up cc: other possibly interested organisational units of the KBA and/or cybersecurity@kba.de, or to inform the respective units directly if it can be assumed that the information may also be of interest to them[3].

(3) Alternatively or in addition to written reporting, the manufacturer may propose other forms of reporting (see also “Application of the Rules for designation/recognition for technical services (categories A, B, D) for testing in the context of the KBA-type approval procedure according to UN-R 155/156”, Section B 2.2).

(4) The report to the KBA does not replace the reporting obligation to the TS. Communication between the manufacturer and the relevant TS shall be agreed separately between them.

(5) In the case of digital communication, the sender must be clearly identifiable and the information must be protected against falsification. The used procedures must be agreed with the KBA.

(6) Regular reports from the manufacturer serve to demonstrate the effectiveness of the CSMS/SUMS and allow the TS and the KBA to comply with their surveillance obligations. Both bodies shall be notified at least every 12 months from the date of issue of the certificate of conformity. They contain summarised information for the reporting period[4]. If a shorter reporting period has been agreed, quantitative information shall be provided cumulatively for the whole year.

In order to compile and submit the report, the manufacturer shall be granted a grace period of three months.[5]

(7) Ad hoc messages on internal and external events must[6] be addressed to the KBA after the relevance has internally been checked. In cases of doubt, in particular where there may be significant events, a preliminary notification must be made prior to the completion of the check. The manufacturer should address ad hoc notifications in its sole discretion and at the request of the TS in the case of its legitimate interest.

---

2 Digital signatures and similar measures to protect integrity and authenticity are permitted, provided that the separation of the data is not hindered.
3 Does not apply to reports to be delivered on a regular basis
4 Also applies to events already reported. Details do not have to be repeated.
5 Alternatively, this allows reporting up to 3 months after the date or completion of the reporting period up to 3 months before the date (with the following reporting period not exceeding 12 months).
6 Events may include, for example: Attacks, essential non-conformities or other weaknesses in the management system, subsequently identified significant gaps in risk analysis, vulnerability or malfunction of products related to UN-R 155/156, etc.

(8) The reports and notifications shall be delivered regardless of any planned or already made requests for change of the certificate for the management system or type-approval.

(9) Management system and approval object may be reported separately to the KBA; if necessary, the information will be forwarded internally to the respective units of the KBA.

(10) All parties concerned shall treat the information provided confidentially[7].

(11) If certain detailed information cannot be issued by the manufacturer for confidentiality reasons, appropriately neutral information and references to the detailed information are permitted. The KBA will check and evaluate detailed information in a suitable manner agreed with the manufacturer.

(12) The manufacturer is expected to also report information on newly detected vulnerabilities, even if corrections and corrective actions have already been implemented for them and their effectiveness can be demonstrated. Depending on the importance, this may require an ad hoc notification. This information is evaluated with regard to the effectiveness of the measures.

(13) Generalised and anonymised by the KBA statements may be made public by the KBA in an appropriate form (e.g. in working groups, at conferences, in exchange of experience, etc.). The aim is to ensure that “best practice” is generalised and that incidents or near incidents may not be repeated. In any case, the manufacturer concerned is informed before information is made public (regardless of whether it is anonymised or not anonymised information). The manufacturer may require that information not be communicated publicly unless required by law.

(14) The effectiveness of reporting is regularly evaluated by the KBA with the participation of all interested parties. As a result, adjustments may be made.

(15) Unless otherwise stated here, for the time being the KBA will make no further requirements for reporting. However, the manufacturer should coordinate the intended type of CSMS/SUMS reports with the KBA (Dresden).

(16) This document sets out minimum requirements. Claims by the TS, other units of the KBA or other authorities to the manufacturer that go beyond these guidelines shall remain unaffected.

(17) Special requirements shall also remain unaffected in the context of the verification of conformity of production or market surveillance. Where notifications could be relevant to several units of the KBA, the manufacturer is recommended to send them in copy to all affected units.

(18) The reporting obligation is also subject to cybersecurity-relevant events, incidents and results of monitoring related to the backend, service and similar solutions necessary for the operation of the approval object.

7 Reporting under UN-R 155

7.1 Regular report in accordance with UN-R 155 Section 7.4.1

7.1.1 General

If appropriate, quantitative data should preferably be represented graphically. The minimum content defined in 7.1.2 applies. The manufacturer agrees with the KBA (Dresden) regarding the level of detail. Trends compared to previous reporting periods should be presented.

[7] This does not preclude the necessary exchange of information between KBA-BSI and TS.

7.1.2 Minimum content of the report to the KBA (Dresden)

7.1.2.1 In relation to the CSMS

- Planned actions for the reporting period, information on implementation, additional measures[8]
- Results (subdivided by manufacturer's categories if applicable) including significant corrective measures
- Assessment of the adequacy and effectiveness of
  - Internal monitoring programme (including staff, other resources, type/frequency/extent of actions, etc.)
  - Corrective actions

7.1.2.2 In relation to the approval object for production and post-production phase respectively

- Type of event[9]
- Number of events per event type
- Results of root cause analysis and corrective actions for each event
- Assessment and confirmation of the adequacy and effectiveness of corrective actions

7.1.2.3 Other information

- Planned and realised significant changes to the structure and processes of the CSMS as well as to the risk analysis
  - Description of the activity
  - Objective and justification
  - Possible impact on the relevant approval objects and other assets to be protected with regard to their cybersecurity
- Assessment of possible influences of new type-approvals and modifications of type-approvals on the CSMS

7.1.2.4 Summary assessment of the adequacy and effectiveness of the measures implemented

7.2 Ad hoc message

7.2.1 Need

Ad hoc notifications are necessary for[10]

- Events that could have a direct impact on the validity of CSMS certificate or type-approval.
- Essential non-conformities of the CSMS.
- Successful and attempted attacks.

7.2.2 Content of the message (if reasonable and possible)

- Date of the event[11]
- Description of the event
  - Type/category of event
  - Affected elements of the CSMS or approval-relevant elements of the E/E architecture
  - Attack paths and scenarios, possible target(s)

8 e.g. system/process/security audit, management reviews, certification audits by the TS, etc.
9 In particular, information relating to Sections 7.2.2.2 g and h of UN-R 155

10 see also section 6 digit (13)
11 unless known, the date of notification

    - Real and possible consequences, severity assessment
- Root cause analysis
- Immediate and other (planned) measures
- Planned measures to check effectiveness
- Event repeated by nature (yes/no)
- Adaptation of the catalogue of actions, of the risk analysis for the approval object (and, where applicable, type-approval) or CSMS (and, where applicable, the certificate of conformity for the CSMS) required/done (yes/no)[12]
- Manufacturer's internal process number
- If applicable, registration feature in external systems (e.g. CVE number)

7.3 Additional information

For the purpose of the international type-approval procedure, the KBA asks to inform in the context of the regular or ad hoc notifications also about

- Other newly identified potential threats and problems that could potentially be of relevance across manufacturers (e.g. apparently accumulating real or attempted attacks, even if they have already been reported immediately upon becoming known (ad-hoc))[13]
- External inquiries that may be relevant to the KBA[14]
- Use of the CSMS certificate for approvals by other approval authorities

8 Reporting under UN-R 156

8.1 Minimum content of the regular report to the KBA (Dresden)

8.1.1 Internal monitoring of the management system

- Planned actions for the reporting period, information on implementation, additional measures[15]
- Results (subdivided by manufacturer's categories if applicable) including significant corrective measures
- Assessment of the adequacy and effectiveness of
    - Internal monitoring programme (including staff, other resources, nature/frequency/extension of actions, etc.)
    - Corrective actions

8.1.2 Other information

- Planned and realised significant changes to the structure and processes of the SUMS as well as to the risk analysis
    - Description of the activity
    - Objective and justification
    - Possible impact on the relevant approval objects and other values to be protected with regard to the security of software updates
- Assessment of possible influences of new type-approvals and modifications of type-approvals on the SUMS

[12] please justify "No"
[13] even if no customisation of your own CSMS was necessary
[14] in particular, requests from other approval or market surveillance authorities and other requests relating to the certificate, the approvals granted on the basis thereof and the procedure for issuing and supervising the certificate and approval as a whole
[15] e.g. system/process/security audit, management assessments, certification audit by the TS, etc.

8.2 Ad hoc message

8.2.1 Need

Ad hoc notifications are necessary for[16]

- Events that could have a direct impact on the validity of SUMS certificate or type-approval.
- Essential non-conformities

8.2.2 Content of the message (if reasonable and possible)

- Date of the event[17]
- Description of the event
  - Type/category of event
  - Affected elements of the SUMS
  - Real and possible consequences, severity assessment
- Root cause analysis
- Immediate and other (planned) measures
- Planned effectiveness control measures
- Event repeated by nature (yes/no)
- Adaptation of the risk analysis for the approval object (and, where applicable, type approval) or SUMS (and, where applicable, the SUMS certificate of conformity) required/performed (yes/no) [18]
- Manufacturer's internal process number

8.3 Additional information

For the purpose of the international type-approval procedure, the KBA asks to inform in the context of the regular or ad hoc notifications also about

- External inquiries that may be relevant to the KBA19
- Use of the SUMS certificate for approvals by other licensing authorities

[16] see also section [6] digit (13)
[17] unless known, the date of notification
[18] "No" please justify
[19] in particular, requests from other licensing and market surveillance authorities and other requests relating to the certificate, the authorisations granted on the basis thereof and the procedure for issuing and supervising the certificate and authorisation as a whole

Legal notice

Publisher:
Kraftfahrt-Bundesamt
24932 Flensburg

Internet: www.kba.de

Special information and advice:

Phone: +49 461 316-2600
E-mail: cybersecurity@kba.de

Revision 1.0 final, Version: 27.06.2022

Picture Source: KBA/www.shutterstock.com (© Bauer Alexander)