Purpose

This regulation is a summary of the requirements of SOR Libchavy spol. s.r.o. on suppliers and goods that have been evaluated as CySe relevant. The purpose of, is to meet the requirements of the CSMS (Cyber Security Management System) defined by the UNECE R 155 regulation.

List of terms

CySe Cyber Security

CSMS Cyber Security Management System

SUMS Software Update Management System

CySe component CySe relevant goods (control units, converters, sensors, …)

CySe definition of relevant goods (components)

**CySe relevant goods are defined by SOR.** In general, any goods that are relevant from a cybersecurity perspective. Goods are CySe relevant if:

* it is an electronic component connected to the A bus
* may affect human health or life (e.g. creating a hazardous situation or affecting driving) or the environment or confidential information OR
* has the possibility of an external connection (connector, internet, WIFI).

CySe REQUIREMENTS FOR SUPPLIERS AND GOODS

CySe requirements for suppliers

Prior to the first delivery of a CySe component, and as part of the periodic supplier evaluation, the SOR supplier shall provide the following documentation to demonstrate a sufficient approach to ensuring the cybersecurity of their organisation:

1. CySe certificate of the organisation, e.g. **UNECE R 155, ISO 27001, ISO 21434**or **TISAX** issued by an authorised person; or
2. proof of the organisation's classification as an obliged person under Regulation Directive (EU) 2022/2555 of the European Parliament and of the Council - abbreviated as "**NIS2**"; or
3. completed [**CySe supplier questionnaire**](https://www.sor.cz/wp-content/uploads/2024/04/MPQ-840-2-P%C5%99%C3%ADloha-4-CySe-questionnaire-for-suppliers.docx) containing an affidavit. SOR reserves the right to verify the truthfulness of the affidavit by conducting a customer audit of the supplier,
4. and at the same time [**CySe DIA Cybersecurity Interface Agreement**](https://www.sor.cz/wp-content/uploads/2024/04/MPQ-840-2-P%C5%99%C3%ADloha-2-DIA.xlsx), or own version of the agreement.

During the annual evaluation of suppliers, it is verified that the supplier still meets the above-mentioned conditions. On behalf of SOR, this evaluation and contact with the supplier is carried out by the Purchasing Department (in cooperation with the CySe Manager).

The supplier is also obliged to:

1. immediately notify SOR of the occurrence of a serious **vulnerability** or **cyber incident** or the **release of a critical update**(potentially affecting passenger security) by email: notification@sor.cz.

CySe requirements for purchased components

In case of a CySe component, the supplier is obliged to deliver:

1. **CSMS certificate** for goods according to UNECE R 155 issued by an authorized person (if any);
2. current results of **TARA** analysis (we prefer to use the methodology according to ISO/SAE 21434):
* risks arising from TARA analysis,
* **technical measures** to mitigate their negative impacts;
1. component:
* clearly **identify a component** if it is intended for testing or development purposes,
* for serial production vehicles, **use only the OBD socket and the UDS protocol** for CAN diagnostics and software updates,
* **penetration test results** including fixes of findings, if available;
1. software:
* **manuals for diagnostic software**,
* safe **procedures for updating software** or unit parameters,
* secure **access to current versions of software**,
* clearly **distinguish software**intended for vehicle operation on the road from unsafe or test software,
* ensure the **immutability of software during updates** (e.g. on-line updates, e-signature or checksum, encryption, etc.),
* **software test** results (e.g. CVE and CVSS or comparison with [nvd.nist.gov](https://nvd.nist.gov/vuln/search));
1. encryption:
* components and SW protected by secure cryptographic protocols, ciphers and hashing functions, i.e. without known vulnerabilities (according to NÚKIB or NIST) and regularly (at least once a year) compare this status,
* if other (unapproved) encryption algorithms are used, the SOR must be informed,
* current links:
	+ [NÚKIB](https://nukib.gov.cz/download/publications_en/Minimum_Requirements_for_Cryptographic_Algorithms_final.pdf),
	+ [NIST](https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines);
1. in the case of an ECU, a **list of queries** to which the ECU responds via CAN:
* ECU hardware version (model number or product number),
* ECU serial number,
* software version,
* Integrity Validation Data;
1. the **end date of support for** the goods (development and production of the goods/components).

If the supplier is unable to deliver point 2, the cooperation of SOR (Director of Purchasing and Logistics, CySe Manager) and the supplier's technical experts is required. For this, the supplier shall prepare in advance:

1. technical documentation of the component including block connection diagram, communication interface, and operational states.
2. description of the safety mechanisms and measures used,
3. the provision of sufficient staff and expertise for the consultation and a proposal for its timing.