On-site inspection elements and overall guidance

Date: Feb. 2025

Version: 1.03

Objectives:

The main purpose of the on-site inspection is 1) to check if all the Security related RMI transactions relate to legitimate business activities; and 2) if the requirements are complied with that are set out in the SERMI scheme and/or legislation, applicable for IO/RSS organisations and employees.

This whitepaper provides guidance for the on-site inspections and outlines what shall be checked. This paper is non-exhaustive and non-binding but is recommended to be followed.

Scope

IO/RSS enterprises and their employees

Compliance with the relevant section in the SERMI scheme:

The IO/RSS shall meet all requirements set out in Appendix 3 of Annex X to Regulation (EU) 2018/858[1] in order to work with security-related RMI and comply to the applicable sections in the SERMI scheme:
The CAB must check that the IO/RSS and the IO/RSS employees meet all the requirements set out in chapter 6.3, 6.4 and 6.5 of the scheme document.

On site inspections requirements:

The CAB visits the IO/RSS and carries out an on-site inspection by verifying compliance with the criteria mentioned underneath and in point 6.3.5. of the SERMI scheme. The CAB may request the assistance of market surveillance authorities from the Member State they are established in, for the purposes of an on-site inspection.

Depending on the outcome of the on-site inspection, the IO/RSS company approval is either confirmed or revoked. Following a negative result and provided the deficiencies are only minor, the CAB can allow the IO/RSS to correct these minor deficiencies, as long these are done in accordance with what is outlined below and in accordance with point 6.3.6 of the SERMI scheme.

[1] OJ L 151 14.6.2018, p. 1

A final negative result of the IO/RSS company inspection will lead to in the revocation of the IO/RSS approval, the IO/RSS employee authorisations, and the IO employee digital certificates by the TC.

Prior to approving an IO/RSS during any on-site inspection (during the approval validity period), CABs shall check the following:

1 Documented ownership of IO/RSS, name of managing director;
2 The list provided by the IO/RSS of employees to be authorised;
3 The IO has informed the CAB in case of any termination of employment of any of their authorised employees within the period that has been set in the scheme.
4 Information about the responsibility and the function of the employees referred to in point 2;
5 Whether the IO/RSS has a liability insurance with a minimum amount of coverage (of 1 million Euro) for bodily injury and (0.5 million Euro) for property damage;
6 Whether the approval of the IO/RSS has been revoked for reasons of misuse;
7 Whether the IO/RSS has provided proof of activity in the automotive area;
8 Whether the declaration certifying that the IO/RSS pursues a legitimate business activity is available and properly signed.
9 Whether it has been confirmed during an on-site inspection, that the IO effectively conducts a legitimate business activity; based on the documents presented, clearly demonstrating that the company pursues legitimate business activities this includes point 6.3 of the Delegated Regulation EU 1244/2021 and has not been convicted of any relevant criminal activity;
10 Whether the IO/RSS and/or the IO/RSS employees have a clean criminal record.
11 Whether there is a declaration signed by the IO/RSS legal representative that compliance with the formal requirements is ensured for all operations related to vehicle security.
12 Whether the data storage, data processing of consumer data and their privacy rights are respected in compliance with the General Data Protection Regulation (EU) 2016/679[2].

For the IO/RSS Employee the following additional checks shall be carried out:

1 That the employee concerned did not have a previous authorisation which has been revoked because of misuse of that authorisation;
2 That there is a valid employment agreement / work contract in accordance with the national rules between the employee concerned and the accredited IO/RSS employer concerned;
3 That the employee concerned has a valid country specific identity card or equivalent identification document;
4 The employee didn't store any records of security related RMI, downloaded from the vehicle manufacturer RMI [for any other purpose than for direct repair or maintenance of the car in progress];
5 The employee hasn't lost, shared or misused their digital security certificate without informing the CAB within 24 hours of such loss or misuse;
6 Investigate whether there isn't any offence or misconduct during the certificate validation period that:
    a. has not been reported to the CAB and contained by the IO/RSS;
    b. that has been committed by the IO/RSS authorised employee;
    c. that concerns security related RMI breaches of the legal or SERMI scheme requirements.

[2] OJ L 119, 4.5.2016, p. 1–88

Applicable for IO-role only

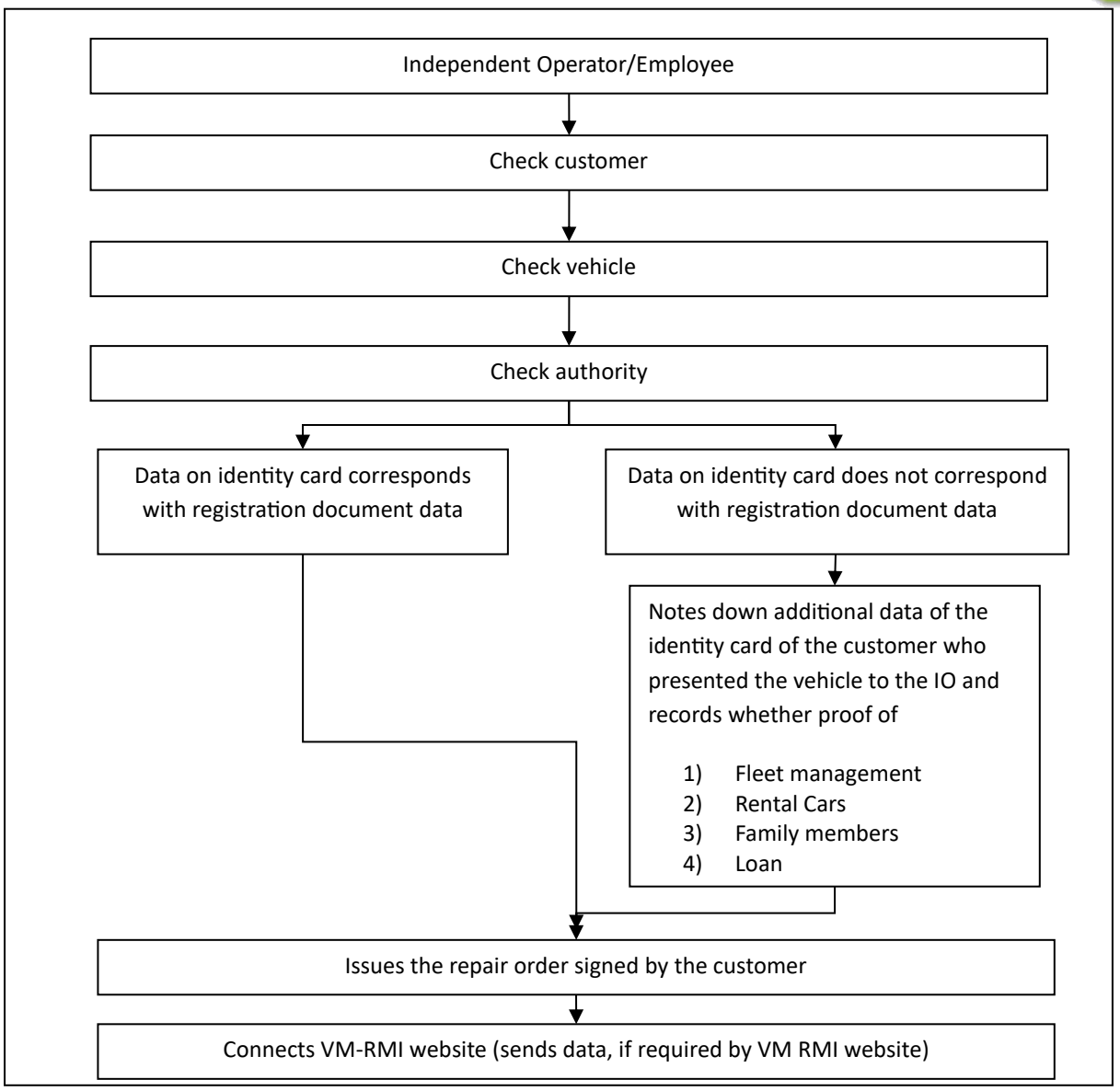
Check the repair order or invoice (Procedural requirements for security-related operations)

To properly identify the legitimacy of the customer request to repair or maintain the vehicle's security system, including it parts, equipment and control as well as the legal ownership of the vehicle, the repair order/invoice shall contain at least the following data and information:

- validation that Identity owner, vehicle registration papers and authority to carry out the work are verified;
- date;
- registration Number to identify the vehicle (the VIN details);
- Make, Type, Variant, Version of the vehicle;
- Actual odometer reading;
- Signature of the customer (vehicle owner or the person who brings the vehicle to the IO).

Signed repair orders/Invoices must be kept for a minimum of 5 years by the IO. Digital copy is allowed for storage purposes.

The figure underneath describes the procedure for IO and employee:


Independent Operator/Employee
Check customer
Check vehicle
Check authority
Data on identity card corresponds with registration document data
Data on identity card does not correspond with registration document data
Notes down additional data of the identity card of the customer who presented the vehicle to the IO and records whether proof of
1) Fleet management
2) Rental Cars
3) Family members
4) Loan
Issues the repair order signed by the customer
Connects VM-RMI website (sends data, if required by VM RMI website)