Scheme for accreditation, approval and authorisation to Access Security-related Repair and Maintenance Information (RMI)

SERMI operations group

February 2023

Table of contents

1 Scope

This scheme is the basis for accreditation, approval and authorisation of Independent Operators(IO) and Remote Service Suppliers(RSS) requiring access to security-related vehicle RMI and services.

It specifies in detail the process and the bodies required to approve and authorise IOs and RSS's to be granted access to security-related vehicle RMI according to the following Regulations:

- Regulation (EU) No. 2018/858 as amended by (EU) 2021/1244

Parenthetical references have been added pointing to corresponding sections in the corresponding regulation.

For light passenger and commercial vehicles (Euro 5 and Euro 6):

- Regulation (EC) No. 692/2008 as amended by (EU) 566/2011

The scheme owner is the association "Forum for Access to Security-Related Vehicle Repair and Maintenance Information", in abbreviated form "SERMI".

2 Normative references

The following referenced documents are indispensable for understanding and applying this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 18541-1:2014, *Road vehicles - Standardized access to automotive RMI — Part 1: General information and use case definition*

ISO 18541-2:2014, *Road vehicles - Standardized access to automotive RMI — Part 2: Technical requirements*

EN ISO/IEC 17011:2017, *Conformity assessment - General requirements for accreditation bodies accrediting conformity assessment bodies*

EN ISO/IEC 17020:2012, *Conformity assessment - Requirements for the operation of various types of bodies performing inspection*

Regulation (EU) No 910/2014 *of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market*

Regulation (EU) No 2015/1502 *of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market*

ETSI TS 102 042, *Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates (this standard is only applicable when and if Qualified Certificates for eSigning are used)*

ETSI EN 319 410 - *General Policy Requirements for Trust Service Providers*

3 Terms, definitions, symbols and abbreviated terms

3.1 Terms and definitions

3.1.1 Accreditation

attestation by a national accreditation body (NAB) that a conformity assessment body (CAB) meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity. As defined in Article 2, point 10 of Regulation (EC) No 765/2008.

3.1.2 Approval inspection certificate

'approval inspection certificate' shall mean the certificate requested by the CAB (and issued by the Trust Centre) to IOs/RSSs complying with the approval criteria set out in this document and which confirms that those IOs/RSSs are approved and that IO/RSS employees can request the authorisation to access security-related RMI.

3.1.3 Authorisation

process based on the inspection performed by the CAB that assesses an individual employee of an approved IO/RSS company is entitled to be given access to security-related RMI. The individual employee will be allocated a security token containing a personal digital certificate and a PIN issued by a designated Trust Centre (TC).

3.1.4 Authorisation inspection certificate

'authorisation inspection certificate' shall mean the digital certificate issued by the CAB to IO/RSS employees complying with the authorisation criteria set out in this document and which confirms that those employees are authorised to access security-related RMI on the website of a vehicle manufacturer.

3.1.5 Digital certificate

'digital certificate' shall mean a digital certificate which requires a digital signature of the issuing Trust Centre to bind a public key to the identity of the IO/RSS employee in accordance with the standard ETSI EN 319 411-1.

3.1.6 Certification database

'certification database' shall mean a database held by the respective Trust Centre to manage the digital certificate validity and the identifiers of authorised IO/RSS employees.

3.1.7 Security token

'security token' shall mean a device that allows a secure authentication of an IO/RSS. Where a device is Personal Data Storage Unit with Multiple Factor Authentication (MFA) associated with a digital certificate stored on a hardware device.

3.1.8 Security-related repair and maintenance information

'security-related repair and maintenance information' or 'security-related RMI' shall mean the information, software, functions and services required to repair and maintain the features included

in a vehicle by the manufacturer to prevent the vehicle from being stolen or driven away and to enable the vehicle to be tracked and recovered.

Vehicle manufacturers shall design the features to prevent vehicles from being stolen in accordance with UN-ECE Regulation 116 on uniform technical provisions concerning the protection of motor vehicles against unauthorised use. They shall design these features in such a manner that it does not render ineffective the right of independent operators to access repair and maintenance information for features that are not security-related.

3.1.9 Authorisation database

'authorisation database' shall mean a database held by the respective Trust Centre and which contains the authorisation details of the pseudonymised authorised IO/RSS employees and the registration of approved IOs/RSSs. Identification of the IO/RSS and IO/RSS employees can only be done by the respective CAB.

3.1.10 The European co-operation for Accreditation (EA)

'European co-operation for Accreditation' or 'EA' shall mean the body recognised by the Commission in accordance with Article 14 of Regulation (EC) No 765/2008 and which is responsible for the development, maintenance and implementation of accreditation in the Union.

3.1.11 The National Accreditation Body (NAB)

the single body appointed in each member state according to Regulation (EC) No 765/2008

3.1.12 The Conformity Assessment Body (CAB)

The body responsible for inspection of IOs/RSSs and their respective IO/RSS employees and for requesting the digital certificates (and issued by the Trust Centre) according to this scheme, so that IOs/RSSs and their respective IO/RSS employees can be approved and authorised to engage in security in the automotive sector. The CAB is also responsible for investigating claims of misuse and for communicating the result to the TC in case the authorisation and approval should be revoked. The CAB shall be free of any conflict of interests (type A), in particular as regards economic, personal or family links with any stakeholder using or providing RMI.

3.1.13 Independent Operator (IO)

IO company according to the definition given in Regulation (EC) No 2018/858 that submits an application to the CAB for approval to engage employees in security-related repair and maintenance information. An IO company is a workshop or a remote service supplier.

3.1.14 IO legal representative

natural person empowered to legally represent the IO in all aspects of the access to vehicle RMI.

3.1.15 IO employee

'IO employee' shall mean the employee of an approved IO who, upon authorisation by the CAB, will have access to security-related RMI.

3.1.16 Remote Service Supplier (RSS)

Within the scope of SERMI a RSS is a service provider offering remote technical services to an IO based on VM's security-related repair and maintenance information, performing remotely the programming or fitting activating of parts and equipment on a vehicle. The requirements and responsibility of the Remote service supplier are similar to the IO.

3.1.17 RSS employee

‘RSS employee’ shall mean the employee of an approved RSS who, upon authorisation by the CAB, will have access to security-related RMI. The requirements and responsibility are similar to the IO employee.

3.1.18 RSS legal representative

natural person empowered to legally represent the RSS in all aspects of the access to vehicle RMI. The requirements and responsibility are similar to the IO legal representative.

3.1.19 Vehicle Manufacturer (VM)

vehicle manufacturer as defined in Regulation (EC) 2018/858 and whose responsibility within the scheme is to provide access to security-related RMI and functions to all authorised IO/RSS employees and who communicates with the TC to verify the authorisation identity and authorisation status of the IO/RSS employee seeking access.

3.1.20 Trust Centre (TC)

'Trust Centre' or 'TC' shall mean the body designated by SERMI and approved by the Commission and that is responsible for:

(a) providing and managing of the digital certificates and authorisation status of the IO employees and for providing to the CAB the necessary tools/software to invite the authorised IOs/RSSs and IO/RSS employees to create security tokens and digital certificates;

(b) providing a vehicle manufacturer with an authentication and authorisation interface to provide the authorisation status of an IO/RSS employee.

(c) when delivering the digital certificate with MFA the evidence of the identity of the IO/RSS employee, shall be checked directly or indirectly using means which provides equivalent assurance to physical presence. (ETSI EN 319 411-1 REG-6.2.2-16 and the Regulation (EU) No 2015/1502 Article 2.2.2)

(d) providing a chain authorisation for the RSS employee to be able to act officially and will have access to security-related RMI on behalf of an IO employee. Both IOEUID RSSEUID will be send to the VM.

3.1.21 Forum for Access to Security-Related Vehicle RMI (SERMI)

The 'Forum for Access to Security-Related Vehicle RMI' or 'SERMI' means the entity that is in charge of coordinating and advising the Commission on the implementation of the procedures of "accreditation, approval and authorisation for the purpose of accessing" security-related RMI. And is the scheme owner of the SERMI-scheme, as is addressed in the EA rules as scheme ownership. The founding members of SERMI shall represent the stakeholders in the process for access to security-related vehicle RMI.

3.1.22 Relevant Authorities (RA)

‘relevant authorities’ shall mean those public authorities that have a legal mandate to act in the area of vehicle security crime protection, investigation and prosecution.

3.2 Abbreviations

Abbreviation	Definition
ACEA	European Automobile Manufacturers Association
CAB	Conformity Assessment Body
CABUID	Conformity Assessment Body unique identifier
CIRCA	Communication & Information Resource Center Administrator
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
DPA	Data Protection Act
EA	European co-operation for Accreditation
EC	European Community
EN	European Norm
SERMI	Forum for Access to Security-Related Vehicle Repair and Maintenance Information
IO	Independent Operator
IOEUID	Independent Operator Employee Unique Identifier
IOUID	Independent Operator Unique Identifier
MFA	Multi Factor Authentication
NAB	National Accreditation Body
OCSP	Online Certificate Status Protocol according RFC 2560
PIN	Personal Identification Number
PKCS#11	Public Key Cryptography Standard
RA	Relevant Authority
RMI	Repair and Maintenance Information
RSS	Remote Service Supplier
RSSEUID	Remote Service Supplier Employee Unique Identifier
RSSUID	Remote Service Supplier Unique Identifier

SOAP	Simple Object Access Protocol (Authorisation Web Service)
TC	Trust Centre
VM	Vehicle Manufacturer

4 Document overview and structure

An overall description of the scheme and context to access security-related vehicle RMI is given in chapter 5.

The scheme is specified in detail in chapter 6, where the bodies involved in the process are described with regards to their role, responsibilities, institutional legitimacy criteria and functional operation requirements.

Technical scheme implementation requirements are specified in chapter 7.

5 General information

The context of IO/RSS access to security-related RMI consists of two processes. One process is designed to provide the IO/RSS and its employees with an approval and authorisation for access to RMI. The other process depicts the access to security-related RMI in a VM RMI system.

5.1 Approval and authorisation of IO/RSS

The process requires that the NAB in the member states be prepared to accredit CABs according to the scheme proposed in this report which has been validated by the EA. It is also required to have CABs accredited by a NAB.

SERMI shall setup and technically manage the database which will enable NABs to add/update/revoke the CABs in the database, that are originally accredited by them. This database allows read access to other NABs, TCs and competent authorities. The accredited CABs will be published on the website of SERMI for lookup services. See also use case “UC NA3. NAB listing of accredited CABs”.

The IO[1] must apply for approval and employee authorisation inspection to a CAB accredited in the state where the employee resides. Once the inspections for IO approval and for an individual IO employee authorisation are performed with a positive result, the CAB informs the TC. The TC creates an authorisation record and issues security credentials a Multi Factor Authentication (MFA) solution based on a digital certificate containing details that will allow the IO employee to be uniquely identifiable to the VM RMI website. The Multi Factor Authentication solution with the digital certificate is provided to the individual IO employee requested by the CAB and issued by the TC. Registration of the IO employee for access to the VM RMI website and payment by the IO in

[1] IO can be substituted by RSS

accordance with the VM RMI website's Terms and Conditions is required to be able to access security-related RMI as described in the next section.

All digital data transfers between IO/RSS, TC and CAB are done via business to business (B2B) transactions in a timely fashion using secure protocols.

The following figure shows the bodies involved in the scheme and their relationship.

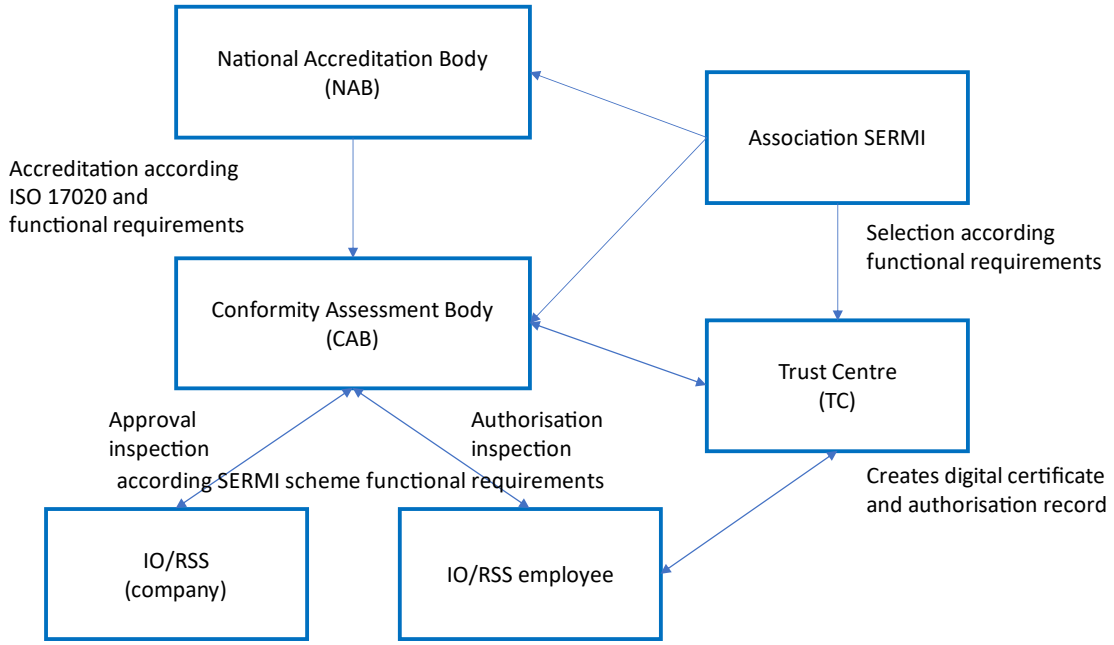

Figure 1: The bodies involved in the scheme and their relationships

The following figure describes the IO approval and IO employee authorisation process. See the relevant Use Cases for further information.

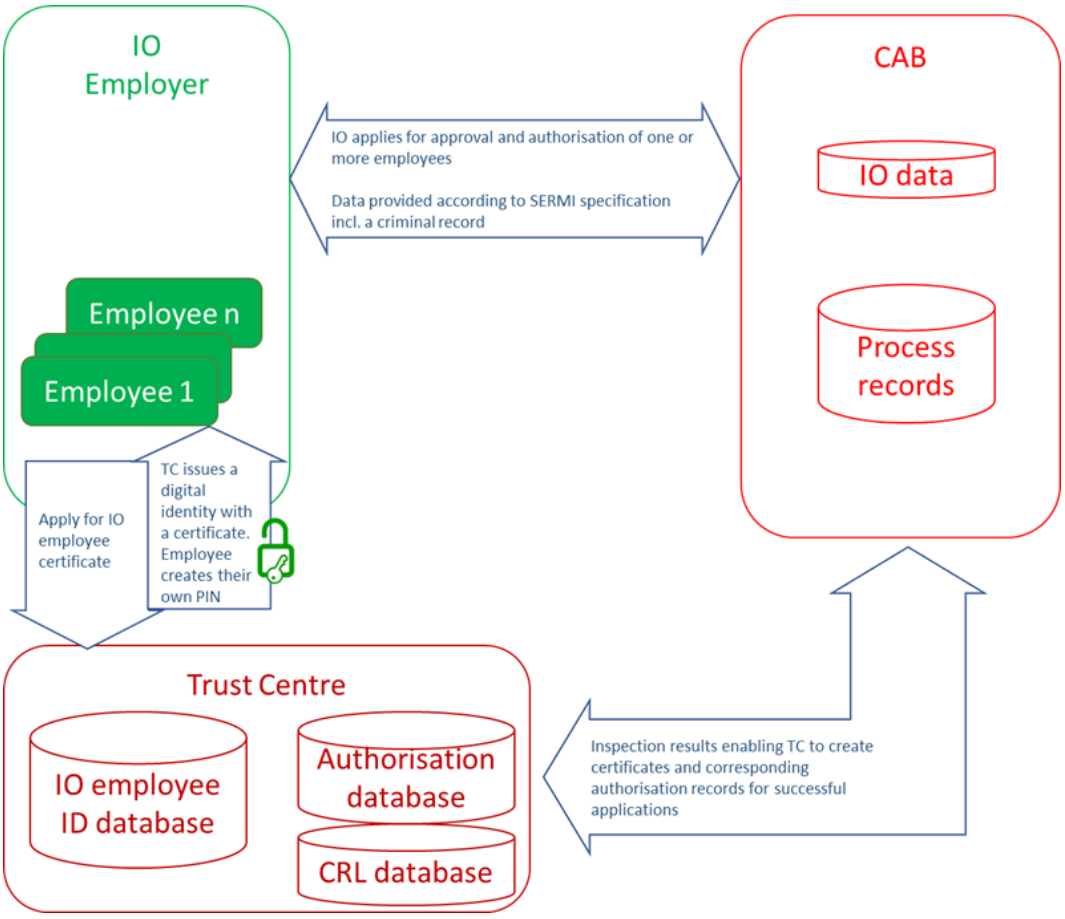

Figure 2: IO approval and IO employee authorisation process

5.2 Overview access to security-related RMI

Access to security-related RMI shall be provided by the VM through its Repair and Maintenance Information (RMI) website provided that the IO/RSS employee is authorised and the IO/RSS on whose behalf the employee is working is approved by the appropriate CAB.

Manufacturers may offer an on-line ordering facility for security-related parts using a specialised application linked to the RMI website, requiring that the IO/RSS employee is authorised and the IO/RSS on whose behalf he is working is approved by the appropriate CAB. Alternatively, security-related parts may be obtained from agents/authorised dealers/3rd party suppliers where currently established authentication procedures are in place (i.e. no digital certificates be required). In any case security-related parts shall be delivered by VMs and or their agents/authorised dealers in a timely manner to the IOs.

Registration of the IO/RSS employee with the VM for access to the RMI website and payment by the IO/RSS for the security functionality is required to be able to login and access security-related RMI.

An authorised and registered IO/RSS employee will, when needed, login to the VM RMI website and request access to the security-related RMI or parts purchasing, module update or key commissioning.

Upon receipt of the request, the VM website will require identification through the IO/RSS employee unique identifier and appropriate authentication and authorisation. Appropriate authentication of

the IO/RSS employee will be done exclusively using the digital certificate. Upon receipt of the digital certificate, the VM RMI website will verify the IO/RSS employee unique identifier and the current status of the certificate and authorisation, by communicating with the appropriate Trust Centre identified in the certificate.

All digital data transfers between IO, RSS, VM, TC and CAB are done via business to business (B2B) transactions in a timely fashion using secure protocols. Once the IO/RSS employee unique identifier and authorisation status has been verified, the VM RMI website shall provide access to the required security-related function.

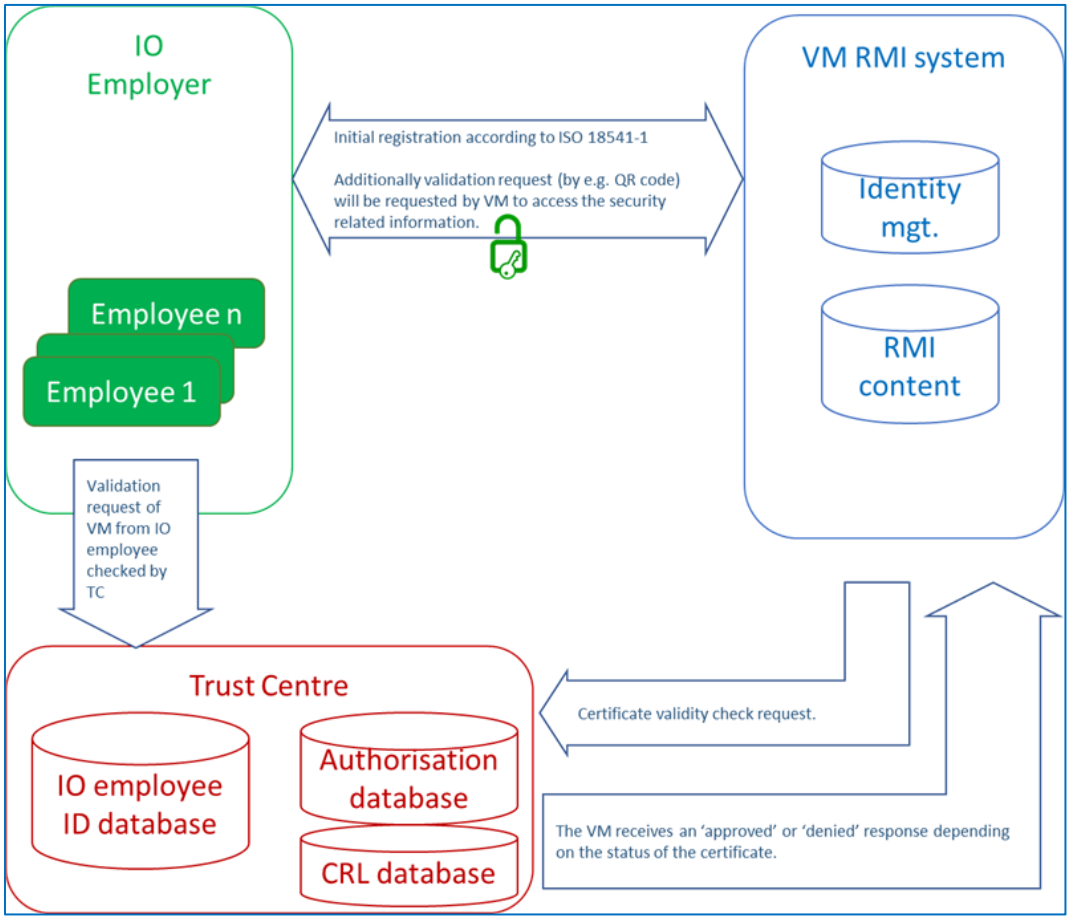

Figure 3: Access to security-related RMI

In case a RSS is requesting access on behalf of an authorised IO, both RSS employee and IO employee unique identifiers will be send to the VM. The current status of the certificates and authorisation, shall be checked by communicating with the appropriate Trust Centre identified in the certificate.

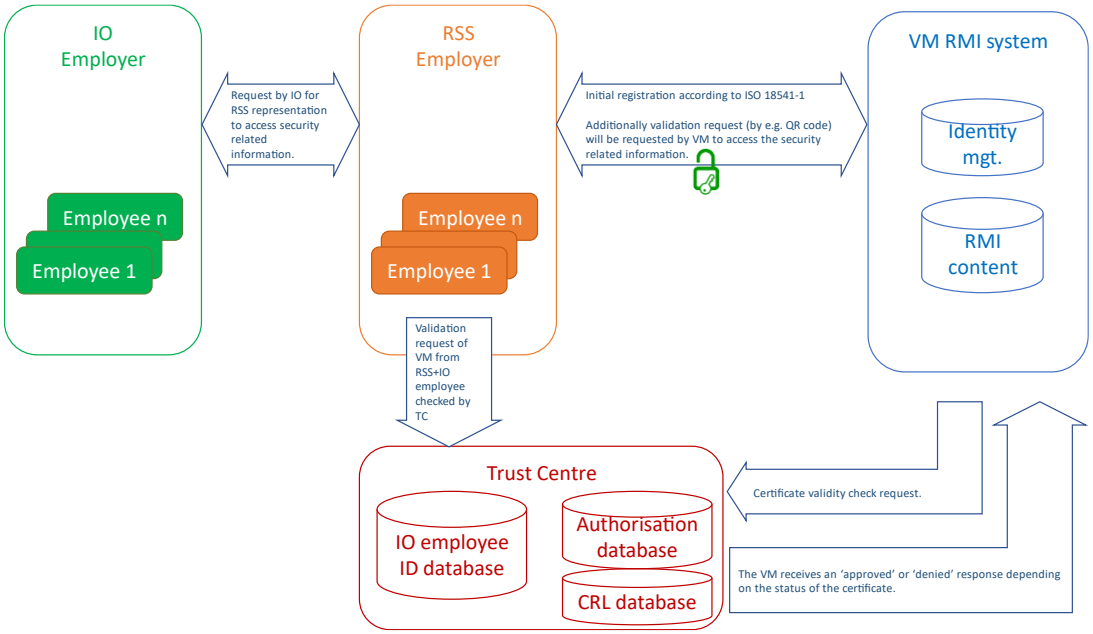

Figure 4: RSS process step to access security-related RMI

6 Scheme specification

6.1 Specification of the SERMI role

The association SERMI is the scheme owner responsible for the definition, operation and maintenance of the accreditation scheme. The association SERMI has received a mandate from the European Commission to become the legitimated body for the Trust Centre (TC) selection process.

6.1.1 Responsibilities and requirements

1) SERMI advises the Commission on requests for changes to the accreditation process.

2) SERMI monitors the implementation of the accreditation process across the Member States and inform the Commission accordingly.

3) SERMI consults the Commission on the creation of the TC selection criteria.

4) SERMI advises the Commission on the introduction of technical implementation guidelines for interaction between the entities involved in the process.

5) SERMI follows the EA's rules on scheme ownership.

6) The members of the SERMI shall be represented by the stakeholders engaged in the process of accreditation, approval and authorisation for the purpose of accessing security-related RMI.

6.1.2 Functional requirements: use cases

UC SE1. Requests for changes to the accreditation process and monitoring the implementation across Member States:

Actor	SERMI members, The Commission
Goal	Actors may make a request to change the scheme.
Use Case Input	A request for changing the scheme to receive security-related RMI.
Use Case Output	Updated scheme to receive security-related RMI where appropriate.
Brief description	SERMI handles requests for scheme changes. Its members evaluate and update the scheme. SERMI advises the Commission on requests for changes to the accreditation process.

UC SE2. Selection of Trust Centre (TC):

Actor	TC, SERMI members, The Commission
Goal	To designate TCs.
Use Case Input	TC´s application to SERMI which shall assess that the TC fulfils all functional and technical requirements.
Use Case Output	Accepted or rejected TC application. Updated selected TC list.
Brief description	SERMI processes requests from TCs applying for selection according to the criteria in point 4.1.2. of Appendix 3 of Annex X to Regulation (EU) No 2018/858, SERMI creates and updates the selected TC list. The Commission is notified.

UC SE3. Setting out the implementation guide for interaction between the entities involved:

Actor	SERMI, Commission
Goal	Use of the implementation guide by vehicle manufacturers and TC to achieve correct implementation of the required communication standards (OCSP, SOAP and/or OpenID Connect).
Use Case Input	Information and known standards.
Use Case Output	Implementation guide providing all required information for the communication interfaces.
Brief description	SERMI provides input to the Commission on the possibility to create and maintain the implementation guide considering enhancing security requirements and improving technologies over time.

6.1.3 Trust centre selection

The TC will be selected by the scheme owner SERMI.

The selected TC shall comply with the standard ETSI EN 319 411-1, fulfil the requirements on electronic signatures laid down in Regulation (EU) No 910/2014 *of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market* and the requirements laid down in article 28.

In addition the TC have the:

- technical and managerial competence, and the financial viability and experience relevant to the accreditation process;
- key personnel that has the skills, experience and availability necessary for the accreditation process;
- ability to operate across Member States;
- quality assurance process in place at operational level.

6.2 Specification of NAB role

The NAB, the single body appointed in each member state according to Regulation (EC) No 765/2008, is responsible for the accreditation of Conformity Assessment Bodies (CAB) as participants in the scheme access to security-related vehicle RMI.

6.2.1 Responsibilities and requirements

NAB responsibilities and requirements are set out in Articles 5 to 12 of Regulation (EC) No 765/2008

6.2.2 Functional requirements: use cases

UC NA1. Accreditation of a CAB

Actor	CAB
Goal	Accredited CAB.
Use Case Input	Application form provided by a CAB to be processed by the NAB.
Use Case Output	CAB is either accredited or not accredited. NAB accreditation report of CAB.
Brief description	Accreditation form provided by the NAB for completion by a CAB. The accreditation form is completed by the organization applying to be a CAB. The NAB assesses that the organization fulfils all requirements specified. • Regulation (EU) No. 2018/858 as amended by (EU) 2021/1244 • SERMI Scheme 2023-02-03 • The accreditation is to ensure that the CAB is assessed for compliance with the standard "Conformity assessment – Requirements for the operation of various types of bodies performing inspection" (ISO/IEC 17020:2012) as inspection body type A. The CAB shall request accreditation according to the rules in Article 5 and Article 7 in Regulation (EC) No 765/2008.

UC NA2. Processing of complaints against CABs:

In accordance with Article 9(4) of Regulation (EC) No 765/2008, National accreditation bodies put in place the necessary procedures to deal with complaints against the conformity assessment bodies they have accredited.

The responsibilities of the NAB include:

(a) decide on the admissibility of the complaint,

(b) where appropriate, ensure that a complaint concerning an accredited CAB is first addressed by the CAB themselves,

(c) take appropriate corrective measures within a reasonable timeframe where necessary,

(d) record all complaints and actions taken, and

(e) respond to the complainant.

During the complaint process through the NAB, all existing IO approvals and all employee authorisations, digital certificates and corrective measures that have been issued by this CAB remain valid.

In case the NAB decides to withdraw the CAB accreditation all IO approvals and related approval digital certificates and all employee digital certificates that have been issued by this CAB ceases to be valid. The CAB subsequently informs the approved IO of that decision. The NAB informs SERMI of that decision.

Actor	IO, TC, VM, relevant authorities.
Goal	To deal with complaints.
Use Case Input	Complaint against a CAB.
Use Case Output	Resolution of a complaint against a CAB.
Brief description	Complaints are resolved at local level between the CAB and the complainant. Complaints that are not resolved at the local level may be referred to the NAB for further consideration in accordance with Article 9(4) of Regulation (EC) No 765/2008.

UC NA3. NAB listing of accredited CABs

Actor	NAB
Goal	NAB shall maintain an updated list of all accredited CABs in the central database.
Use Case Input	Accredited CABs with at least the following information: (a) the name and address of each CAB accredited by that national accreditation body; (b) the Member States in which the CAB is carrying out verification; (c) the date on which the accreditation was granted and the expiry date of the accreditation; (d) any information on administrative measures that have been imposed on the CAB. (e) status of the CAB (active/revoked)
Use Case Output	A country-specific list of accredited CABs. The information shall be publicly available.
Brief description	NAB creates, maintains and publishes a list of all accredited CABs. The information (a), (b), (c) and (e) shall be published on the SERMI website (open access).

6.2.3 Criteria for CAB accreditation

The CAB shall be accredited as a type A inspection body in accordance with ISO/IEC 17020:2012. Option A for the management system requirement shall apply. As a type A inspection body the CAB has to comply with the highest level of independence requirements.

Additionally, the CAB´s capability to meet the responsibilities and requirements described in section 6.3.1 and the functional requirements described in section 6.3.2 shall be assessed by the NAB during the accreditation process.

The personnel in charge of IO/RSS inspections shall have a level of knowledge of the SERMI scheme in the automotive vehicle repair and maintenance business and of the automotive aftermarket specifics that is appropriate for the tasks they are performing.

6.3 Specification of the CAB role

The CAB shall be responsible for the inspection of IO's/RSS's and their respective employees and for issuing approval and authorisation digital certificates in accordance with the SERMI scheme, and for revoking such certificates.

6.3.1 Responsibilities and requirements

1) CABs shall keep the data submitted for the approval of an IO/RSS;

2) CABs shall establish a secure communication channel with the TC and provide the inspection results to the TC in order for the TC to issue the security token with a digital certificate;

3) CABs shall notify IO/RSS employees 6 months before authorisation expires;

4) CABs shall maintain a database containing data submitted for the authorisation of IO/RSS employees;

5) CABs that refuse to approve an IO/RSS or authorise of an IO/RSS employee shall communicate the inspection results concerning the IO/RSS or that employee to the TC;

6) CABs shall only collect and use data required for the approval or authorisation process;

7) CABs shall keep all data relating to IO/RSS and IO/RSS employees confidential and shall ensure that only authorised employees have access to such data;

8) CABs shall provide once a year statistics on the number of approval and authorisations issued and also on the number of refusals to SERMI and the Commission;

9) CABs shall retain secure records of approval and authorisation inspections for a period of 5 years;

10) CABs shall inform all other CABs in the Member State in which it is established about negative inspection results of an IO/RSS;

11) IOs/RSSs and IO/RSS employees that have received a negative inspection result may provide the CAB with additional information correcting minor deficiencies within 15 working days from receiving the negative inspection result. CABs shall accordingly determine whether the inspection result is to be changed;

12) CABs shall notify IOs/RSSs 6 months before their approval expires;

13) CABs shall make random and unannounced on-site checks of IOs/RSSs within the 60 months approval validity period, and subject each approved IO/RSS to at least one random, on-site inspection over the 60 months approval validity period (minimum of 2 inspections: one random and one 6 months before authorisation is due to expire);

14) On the basis of a complaint against an approved IO/RSS or an authorised IO/RSS employee, CABs shall check that the concerned IO/RSS or IO/RSS employee are in compliance with the criteria against which they were respectively approved or authorised. The CAB shall determine during its investigation whether an on-site inspection is required;

15) For the purpose of on-site inspections, CABs may request the assistance of market surveillance authorities from the Member State they are established;

16) CABs shall revoke IO/RSS approvals and IO/RSS employee authorisations where they no longer comply with the criteria against which they were respectively approved or authorised.

The CAB shall accordingly request the TC to suspend and repeal digital certificate of the concerned IO/RSS and IO/RSS employees.

6.3.2 Renewal of the approval

CABs shall, upon request by an IO/RSS or, 6 months prior to the expiry of validity of the approval, make an on-site inspection, and in case of a positive inspection result, renew the approval.

The CAB shall issue a new digital certificate for IO/RSS that fulfils the approval criteria.

The CAB shall assess applications for renewals of authorisations and issue an digital certificate to IO/RSS employees fulfilling the authorisation criteria.

6.3.3 Transfer of inspection

If a CABs accreditation is withdrawn the existing IO/RSS approvals and IO/RSS employee authorisations shall be transferred to an accredited CAB. This CAB is to be selected by the IO/RSS. For this transfer all details of the IO/RSS, IO/RSS employee and all applicable dossiers (inclusive on-site inspection results) will be transferred to the designated CAB(s).

Only valid accredited authorisations shall be transferred. Authorisation which is known to be suspended shall not be accepted for transfer. In the event the CABs accreditation is withdrawn due to incompetence, fraud or misuse of their position the existing accredited authorisations of the IO/RSS and IO/RSS employees will also be withdrawn.

In cases where an IO/RSS and IO/RSS employee have been authorised by a CAB which has ceased trading or whose accreditation has expired, been suspended or withdrawn, the transfer shall be completed within 6 months or on expiration of the inspection whichever is sooner. In such cases, the accepting CAB shall inform the NAB, under whose accreditation it intends to issue the inspection certificate, prior to the transfer.

The accepting CAB shall carry out a review of the validation of the transferring client. This review shall be conducted by means of a documentation review and where identified as needed by this review, for example there are outstanding major nonconformities, shall include a pre-transfer visit to the transferring client to confirm the validity of the certification.

Note: The pre-transfer visit is not an audit.

6.3.4 Functional requirements: use cases

UC CA1. CAB setting up of a business relationship with Trust Centre

Actor	CAB
Goal	CAB sets up a contractual agreement with a selected TC published in the SERMI selected TC list.
Use Case Input	Contract between the CAB and a selected TC chosen from the list of accepted TCs published by SERMI (see UC SE2).
Use Case Output	A signed contract between CAB and TC is issued.
Brief description	CAB contracts a business relationship with one selected TC according to the published SERMI list in order to: a) Create digital certificates and authorisation records via the TC. b) Maintain approval and authorisation status (send out "new" certificate if necessary). A CAB shall only set up a business relationship with one TC.

UC CA2. CAB inspects IO/RSS for approval

Actor	IO/RSS
Goal	Approval of IO/RSS, so that an IO/RSS can name employee(s) for authorisation to be given access to security-related RMI.
Use Case Input	Completed application form as required by the CAB. The application form contains the criteria listed in point 4.3.3. of Appendix 3 of Annex X to Regulation (EU) 2018/858
Use Case Output	Paper certificate with the IO/RSS approval inspection result.
Brief description	IO/RSS legal representative shall send the application form and all necessary documents to the CAB by auditable means. CAB verifies the documents and checks if the IO/RSS fulfil the requirements. If the criteria for IO/RSS approval (point 4.3.3. of Appendix 3 of Annex X to Regulation (EU) 2018/858) are met the CAB shall send the paper approval inspection certificate to the IO/RSS. The CAB notifies by auditable means the other CABs in the respective country if the IO/RSS does not pass the CAB inspection. CAB verifies that the data provided by the IO/RSS is consistent throughout the process. Every IO/RSS employee of an IO/RSS who becomes authorised for access to security information is registered at the same CAB and TC. Note: Every approved IO/RSS can be subjected to unannounced random inspections. This will occur once during the IO's/RSS's approval validity period.

UC CA3. CAB checks IO/RSS on-site

Actor	CAB
Goal	Minimum of one random and unannounced on-site inspection of every approved IO/RSS during the validity period and an IO/RSS requested on-site inspection in the last six months of the validity period to ensure that the information given during application is correct and that the procedural requirements are implemented and practiced in daily operations as stated by the IO/RSS in the application for approval. The inspection carried out in the last 6 months will also be used to determine the renewal of an IO/RSS approval. On the basis of a complaint against an approved IO/RSS or an authorised IO/RSS employee, determines whether an on-site inspection is required.
Use Case Input	Unannounced visit to IO/RSS premises. Visit to IO/RSS premises on IO/RSS request in the last 6 months of the IO approval validity. On the basis of a complaint.
Use Case Output	IO/RSS approval is confirmed or revoked. In case the IO/RSS approval is revoked, the IO/RSS employee authorisations are revoked and the TC is instructed to revoke the corresponding digital certificates. IO/RSS approval is renewed (UC CA 4).
Brief description	CAB visits the IO/RSS and carries out an on-site inspection by verifying compliance with the criteria in point 4.3.3. of Appendix 3 of Annex X to Regulation (EU) 2018/858. CAB may request the assistance of market surveillance authorities from the Member State they are established for the purposes of an on-site inspection. According to the findings during the inspection the IO/RSS approval is confirmed or revoked. The CAB allows the IO/RSS to correct minor deficiencies following the negative result of an on-site inspection in accordance point 4.3.3. of Appendix 3 of Annex X to Regulation (EU) 2018/858. A final negative inspection result has for consequence the revocation of the IO/RSS approval, the IO/RSS employee authorisations and the IO employee digital certificates by the TC. A minimum of 2 inspections: one random and one 6 months before authorisation is due to expire.

UC CA4. CAB inspects IO/RSS for approval´s renewal

Actor	IO/RSS
Goal	Renewal of IO/RSS approval.
Use Case Input	Completed application as required by the CAB. The application form contains the criteria listed in point 4.3.2. of Appendix 3 of Annex X to Regulation (EU) 2018/858. Positive result of an IO/RSS requested on-site inspection by the CAB in the 6 months prior to the approval expiration deadline.
Use Case Output	Paper certificate with the inspection result for renewal of an IO/RSS approval. Expiration of IO/RSS approval, IO/RSS employee authorisation and revocation of the digital certificates in case of a negative inspection result or of a denial of the renewal request.
Brief description	After a time period of 60 months the approval is to be renewed. Prior to expiry of the approval the IO/RSS is notified by the CAB of the pending expiry. This period of notification is six months before the approval ends. IO/RSS requests an on-site inspection by the CAB. The CAB performs the on-site inspection. If the inspection result is negative the CAB revokes the IO/RSS approval and the IO/RSS employee authorisation(s). The CAB instructs the TC to revoke the IO employee digital certificate. IO/RSS sends all documents by auditable means to the CAB two months before the approval expires. CAB verifies the documents and checks if the IO has already been approved or rejected by another CAB. CAB verifies compliance with the concept of legitimate business activity set out in the second paragraph of point 6.3. of Annex X to Regulation (EU) 2018/858. CAB may be assisted by the market surveillance authority from the Member State it is established. If the criteria for IO/RSS approval (see point 4.3.3 of Appendix 3 of Annex X to Regulation (EU) 2018/858) are met the CAB sends the approval inspection paper certificate to the IO/RSS. The CAB notifies by auditable means, the other CABs in the respective country if the IO/RSS does not pass the CAB inspection. CAB verifies that the data provided by the IO/RSS is consistent throughout the process.

	Every employee of an IO/RSS who becomes authorised for access to security information following the authorisation inspection described in use case CA6 is registered at the same CAB and TC.

UC CA5. CAB maintenance of IO/RSS data

Actor	IO/RSS
Goal	IO/RSS data to be corrected.
Use Case Input	IO/RSS requests the respective CAB to amend the IO/RSS data. IO/RSS completes the appropriate amendment form and submit it to the CAB.
Use Case Output	Updated IO/RSS data.
Brief description	IO/RSS sends all necessary documents to the CAB by auditable means. CAB checks the documents. If the CAB determines that the request is justified, the data is amended and the CAB issues the modified paper certificate to the IO/RSS.

UC CA6. CAB inspects IO/RSS employee for authorisation

Actor	IO/RSS employee
Goal	Authorisation of an IO/RSS employee(s).
Use Case Input	Completed inspection application form as required by the CAB. The application form complies with the criteria listed in point 4.3.4. of Appendix 3 of Annex X to Regulation (EU) 2018/858.
Use Case Output	Inspection result send by CAB to TC in order for the TC to: 1) issue a Multi Factor Authentication token associated with a digital certificate for this IO/RSS employee, 2) create the IO/RSS employee´s authorisation record in the database.
Brief description	The IO/RSS employee sends the application and all necessary documents to the CAB by auditable means. The CAB checks the documents. If the criteria for IO/RSS employee authorisation (see point 4.3.4. of Annex X to Regulation (EU) 2018/858) are met the CAB informs the TC in order to issue their Multi Factor Authentication token associated with a digital certificate (use case TC1). Every IO/RSS employee seeks authorisation with the CAB that its IO/RSS is registered with the CAB.

	Verification of the accuracy and completeness of information submitted by the IO/RSS on behalf of its employees is covered by ISO 17020:2012 clause 7.1.6.

UC CA7. Pseudonymisation of Personal Data in CAB

Actor	CAB
Goal	Pseudonymisation of personal data from IO/RSS employee(s).
Use Case Input	First name, last name of the IO/RSS employee.
Use Case Output	IO/RSS employee unique identifier to be used as in the digital certificate.
Brief description	First name, last name of the IO/RSS employee is transferred to an IO/RSS employee unique identifier that will be used throughout the whole process for access to security relevant RMI. Only pseudonymised contact information (e.g. OEUID/RSSEUID@example.com, phone number +XX XXXX IOEUID/RSSEUID) will be forwarded to the TC to link the certificate with the IO/RSS employee. The CAB will match this information with the real contact information of the IO/RSS employee. Interaction from TC and IO/RSS employee will be provided via the CAB backend. The use case ensures the processing of personal data is compliant with EU-rules on protecting fundamental rights and freedoms of individuals, as provided in Regulation (EU) 2016/679 and Directive 2002/58/EC.

UC CA8. CAB informs TC in order to issue a digital certificate

Actor	CAB
Goal	To provide the IO/RSS employee with a digital certificate.
Use Case Input	CAB inspection result to TC for an authorised employee.
Use Case Output	A digital identity combined with a digital certificate based on a secure token and a separate PIN for the IO/RSS employee. The IO/RSS employee receives a notification that the digital certificate and authorisation are ready for use and this notification is forwarded by the CAB by auditable means.
Brief description	The CAB sends invite to the IO/RSS employee via the TC to create a digital identity including a digital certificate based on a digital token with personalized PIN.

UC CA9. CAB inspection of an IO/RSS employee for authorisation renewal

Actor	IO/RSS employee
Goal	Renewal of an employee authorisation
Use Case Input	Completed inspection application form as required by the CAB. The application form contains the criteria listed in point 4.3.4. of Appendix 3 of Annex X to the Regulation (EU) 2018/858
Use Case Output	Renewal inspection result of an IO/RSS employee authorisation.
Brief description	The CAB informs the IO/RSS of the date expiry of the employees' authorisation, 6 months prior to the actual date of the expiration of the authorisation. IO/RSS employee sends all documents by auditable means to the CAB 2 months before the authorisation expires. The authorisation inspection process described in use case CA6 is carried out.

UC CA10. CABs maintenance of employee's data

Actor	IO/RSS employee
Goal	The IO/RSS employee data to be corrected.
Use Case Input	Request to the respective CAB to update the IO/RSS employee data. The appropriate form is completed and signed by the IO/RSS employee prior to submission to the CAB.
Use Case Output	Updated IO/RSS employee data.
Brief description	IO/RSS employee sends all necessary documents to the CAB by auditable means. The CAB checks the documents. If the update request affects the data stored in the digital certificate, the CAB informs the TC in order to issue a new digital certificate (UC TC1).

UC CA11. CAB procedure for complaint and appeal processes

Actor	CAB
Goal	The CAB has a documented process to receive, evaluate and make decisions on complaints and appeals; this process complies with the respective national laws.
Use Case Input	Regulations, standards and SERMI scheme.
Use Case Output	Documented process for complaints and appeals.
Brief description	The CAB develops and documents a process for handling complaints and appeals according to EN ISO/IEC 17020:2012 (7.5). Complaints are resolved at local level between the CB and the complainant. Parties wishing to make representation with regard to a perceived scheme issue should be able to contact the respective CAB with all necessary information. CAB puts in place the necessary procedures and resources to carry out an on-site inspection where it determines that is appropriate to assess a complaint. Complaints that are not resolved at the local level may be referred to the NAB for further consideration in accordance with Article 9(4) of Regulation (EC) No 765/2008.

UC CA12. CAB processes a complaint or appeal concerning an IO/RSS approval

Actor	VM, IO, RSS, TC, RA
Goal	CAB processes complaints or appeals regarding an IO/RSS approval. IO/RSS approval shall be revoked or confirmed following the process outcome. Approval database is kept up to date.
Use Case Input	Complaint or appeal with the required information according to the process in UC CA11.
Use Case Output	Rejection of the complaint or appeal. Or Decision to revoke an IO/RSS approval as result of a complaint or appeal process: 1. IO approval revocation documented and IO/RSS approval classified as revoked in approval database. 2. IO employee authorisations revoked.
Brief description	The CAB investigates the complaint or appeal by notably assessing whether the IO/RSS has remained compliant with the criteria of point 4.3.3. of Appendix 3 of Annex X to Regulation (EU) 2018/858 and with the concept of legitimate business activity set out in the second paragraph of point 6.3. of Annex X to Regulation (EU) 2018/858. CAB may be assisted by the market surveillance authority from the Member State where it is established. If the reasons for the complaint or appeal cannot be confirmed the complaint or appeal shall be rejected. CAB determines whether an on-site inspection is required. The CAB notably assesses whether the IO/RSS has remained compliant with the above points. In case the reasons are confirmed the IO/RSS approval shall be revoked. In the event of a revocation the CAB: 1) informs the IO/RSS legal representative that the approval shall be revoked, 2) informs the respective TC in order to immediately document the approval as revoked and to revoke all digital certificates and authorisations from the IO/RSS employees of the respective IO/RSS, 3) inform all CABs in its member state about the revocation.

UC CA13. CAB processes a complaint or appeal concerning an IO/RSS employee's authorisation

Actor	VM, IO employee, IO, /RSS, TC, RA
Goal	CAB processes complaints and appeals regarding an IO/RSS employee´s authorisation. IO/RSS employee´s authorisation shall be revoked or confirmed by the TC following the process outcome. Digital certificate revocation list and authorisation database is updated.
Use Case Input	Complaint or appeal with the required information according to the process in UC CA11.
Use Case Output	Rejection of the complaint or appeal. Or Information of the TC in order to revoke IO/RSS employee authorisation after a complaint or appeal process: 1) IO/RSS employee´s digital certificate registered as invalid. 2) IO/RSS employee's authorisation status updated as invalid.
Brief description	The CAB investigates the complaint or appeal. The CAB notably assesses whether the IO/RSS employee still meets the criteria of point 4.3.4 of Appendix 3 of Annex X to Regulation (EU) 2018/858 or has participated in activities that would not be compliant with the concept of legitimate business activity set out in the second paragraph of point 6.3. of Annex X to Regulation (EU) 2018/858. CAB determines whether an on-site inspection is required. CAB may be assisted by the market surveillance authority from the Member State it is established. If the reasons for the complaint or appeal cannot not be confirmed the complaint or appeal shall be rejected. In case the reasons are confirmed the IO/RSS employee authorisation shall be revoked. CAB informs the respective TC in order to immediately revoke the employee's digital certificate and the employee´s authorisation. The CAB informs the IO/RSS about the IO/RSS employee revocation.

UC CA14. CAB provision of statistics

Actor	CAB
Goal	CAB Monitors approvals and authorisations.
Use Case Input	Result of approval, authorisations and on-site inspections.
Use Case Output	CAB shall provide a report on a quarterly basis in the first year of CAB activity and then annually to SERMI and the Commission(to be published on SERMI website)
Brief description	CAB analyses the results of the approval/authorisation inspection process and provides a report with: • Number of investigations. • Quotient : approvals/applications • Quotient : authorisations/applications • Most common (at least 3) reasons for refusing approval • Most common (at least 3) reasons for refusing authorisation • Number and outcome of on-site checks in the reporting period • Number and outcome of requests for IO/RSS approval revocation • Most common (at least 3) reasons for IO/RSS approval revocation • Additionally SERMI in cooperation with the Commission can add other Key Performance Indicators (KPI)

6.3.5 Criteria for IO/RSS approval by the CAB

Before 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) Information about the responsibility and the function of the employees referred to in point 2;

4) 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;

5) Whether the approval of the IO/RSS has been revoked for reasons of misuse;

6) Whether the IO/RSS has provided proof of activity in the automotive area;

7) Whether the declaration certifying that the IO/RSS pursues a legitimate business activity as referred to in point 6.3. of Annex X to Regulation (EU) 2018/858 has been signed by the IO/RSS and during an on-site inspection whether the IO effectively conducts a legitimate business activity;

8) Whether the IO/RSS and/or the IO/RSS employees have a clean criminal record.

9) Whether there is declaration signed by the IO/RSS legal representative that compliance with the procedural requirements laid down in point 6.3.5 is ensured for all operations related to vehicle security.

6.3.6 Procedural requirements for security-related operations

6.3.6.1 General behaviour

Only IO/RSS employees of the approved IO/RSS, who have been successfully authorised and are in possession of an authorisation inspection and a valid digital certificate issued by the corresponding Trust Centre, will have access to security-related RMI.

The IO/RSS employee shall assume responsibility for the correct use of the digital certificate and PIN.

The IOs/RSSs and their employees shall follow the procedures to deal with the end user device (PC, Laptop, etc.) as specified in ISO 18541-2:2014.

6.3.6.2 Procedure to conduct security-related operations

If an employee carries out a security related software update or needs other security related repair and maintenance information for a vehicle operation, the procedure described in point 6.3.5.3. to 6.3.5.6. and shown in figure 5 shall be followed.

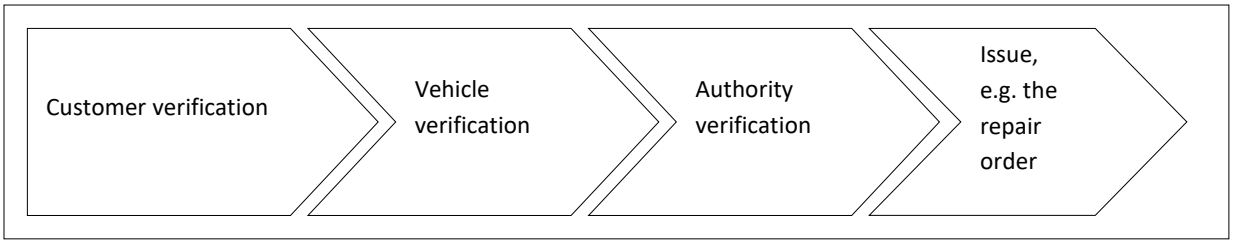

Figure 5: Basic outline of the procedure to conduct a security-related operation

6.3.6.3 Customer ID verification

The IO employee shall verify the identification of the customer that has brought in the vehicle. In case of remote services this check shall be carried out by the IO where the vehicle resides, the IO employee will remain responsible for the customer check.

Possible sources of identification:

➲ Identity card, passport, driver's licence, or roadside membership card

The IO is responsible for recording the identity information in a way which can be audited.

The information provided in figure 6 may be used for this process.

Vehicle registration documents	
Data (Part I)	Field (Part I)
Surname(s) or business name	C.1.1
Other name(s) or initial(s) (where appropriate)	C.1.2

Address in the Member State of registration on the date of issue of the document	C.1.3
Data (Part II)	Field (Part II)
Surname(s) or business name	C.3.1 and C.6.1
Other name(s) or initial(s) (where appropriate)	C.3.2 and C.6.2
Address in the Member State of registration on the date of issue of the document	C.3.3 and C.6.3

Figure 6: Field reference for customer ID verification from the vehicle registration certificate

Where possible, the IO employee notes the following data:

- Name and surname of the customer
- Identity card/passport number and/or number of the roadside member card
- Fleet management or rental car company name
- Contact name of the respective company
- Address of the respective company
- Telephone number of the respective company
- Driver's company identification

This additional information is requested in the circumstances where the customer will not have vehicle registration documents

1) Fleet management
2) Rental Cars
3) Loan

6.3.6.4 Vehicle verification

The IO employee makes sure that the vehicle identification number (VIN) of the vehicle is the same as the VIN on the registration documents.(see figure 7) In case of remote services this check shall be carried out by the IO where the vehicle resides, the IO employee will remain responsible for the customer check.

Vehicle registration documents	
Data (Part I)	Field (Part I)
Vehicle identification number	E

Figure 7: Union codes from the registration documents for the vehicle verification

6.3.6.5 Authority verification

The authority to carry out work on the vehicle shall be established and the mechanism used shall be auditable and will be subject to national law.

The authority of the customer to allow the repair shall be checked by means of an authenticated letter of empowerment for the requested action from the registered owner or an equivalent procedure.

If the authority is not established by an auditable process then the car shall not be repaired until the necessary proof is produced.

Stop processing

In the event of any reasonable grounds for suspicion then the employee should not proceed. If possible and appropriate the situation should be reported to the relevant authorities.

6.3.6.6 Issue the repair order

The next step is to issue the repair order by using a dealer/garage management system (or something similar). The repair order shall contain at least the data from figure 8 and all data used to identify the customer and their authority.

Vehicle registration documents	
Data	Field
Registration number	A
Make	D.1
Type, variant, version	D.2

Figure 8: Union codes from the registration documents for issuing a repair order

The current value of the odometer and the reason for the repair shall be noted and the repair order needs to be signed by the customer (owner and/or the person who brings the vehicle to the IO). The figure 9 describes the procedure for IO and employee.

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

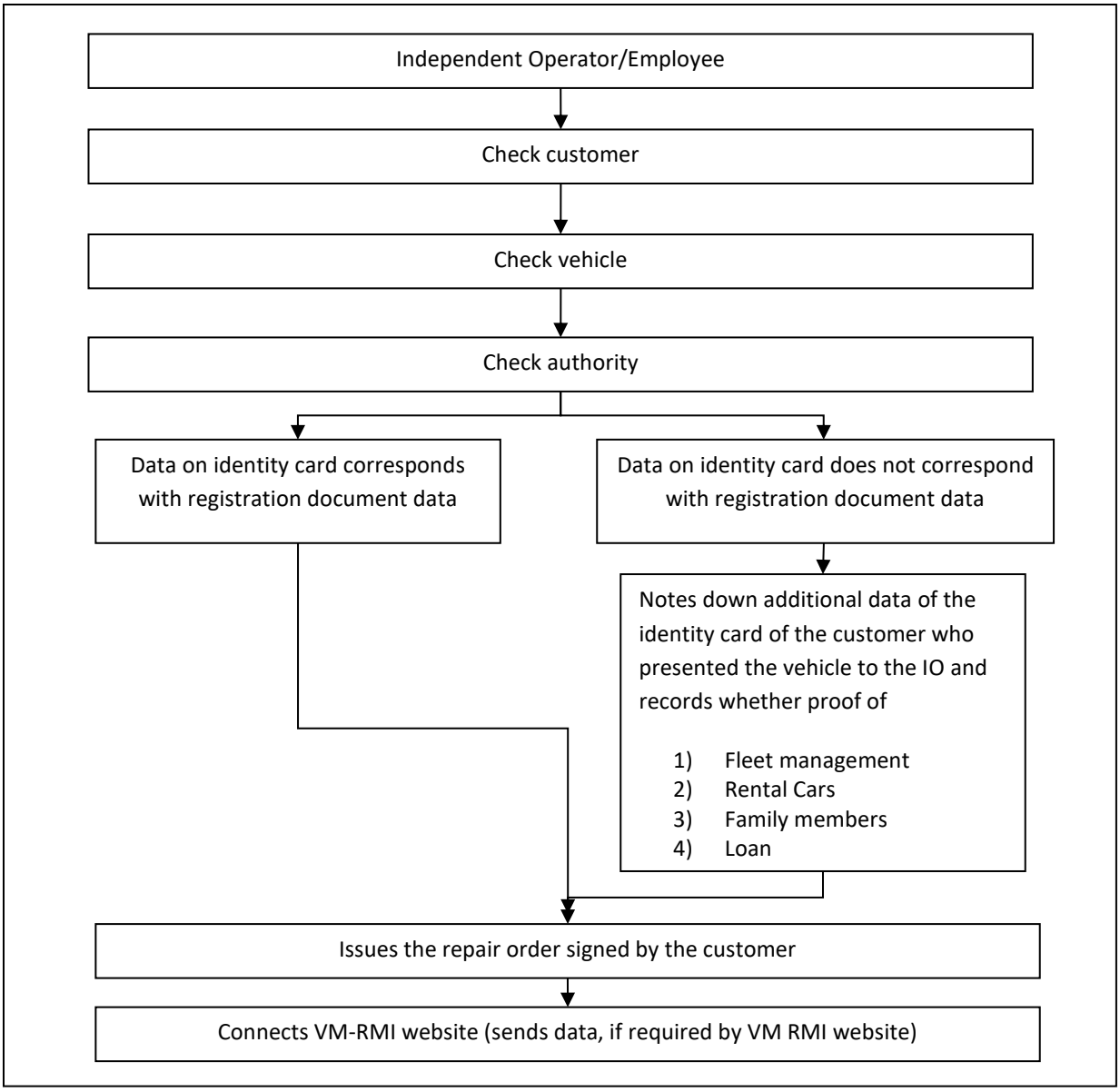

Figure 9: Procedural requirements for IO

Note: In the Commission Notice this is described in UC IO8 'Procedural requirements for security-related operations

6.3.7 Criteria for IO/RSS employee authorisation by the CAB

Before authorising an IO/RSS employee, and during any on-site inspection during the approval validity period, the CAB shall verify the following:

1) That the employee concerned did not have a previous authorisation which have been revoked because of misuse of that authorisation;

2) That the employee has a clean criminal record;

3) That there is an employment agreement between the employee concerned and an approved IO/RSS;

4) That the employee concerned has a valid country specific identity card or equivalent document.

6.4 Role of the IOs/RSSs

The IO/RSS commercial enterprise shall submit an application to the CAB requesting an approval to engage in security-related RMI.

6.4.1 Responsibilities and requirements

1) IOs/RSSs shall request an inspection from their CAB to obtain approval;

2) IOs/RSSs shall inform their CAB about changes in their contact details;

3) The IO/RSS shall inform the CAB when its business is dissolved;

4) IOs/RSSs shall record every security related RMI transactions and operations;

5) IOs/RSSs shall inform their CAB of any termination of employment of any of their authorised employees;

6) IOs/RSSs shall report the relevant authorities any offence or misconduct that has been committed by their authorised employee and that concerns security related RMI;

7) IOs/RSSs shall ensure that their authorised employees only use their own digital certificates;

8) IOs/RSSs shall ensure that all fees relating to their employee's authorisation have been paid.

9) IOs/RSSs shall ensure that their IO/RSS employees are trained for repair activities concerning automotive maintenance, reprogramming and security and safety functions;

10) IOs/RSSs shall request their CAB for an on-site inspection in the six months prior to the expiration of their digital certificate.

6.4.2 Functional requirements: use cases

UC IO1. IO/RSS requests for approval

Actor	IO, RSS
Goal	The IO/RSS shall meet all requirements set out in Appendix 3 of Annex X to Regulation (EU) 2018/858 in order to work with security-related RMI.
Use Case Input	All necessary documents and application form (as provided by the CAB) in auditable format.
Use Case Output	Approval of IO/RSS or non approval of IO/RSS.
Brief description	IO/RSS shall use the SERMI website to obtain a list of accredited CAB(s). The IO/RSS contacts the respective CAB. The IO/RSS receives the application form from the CAB. The IO/RSS fills in the application form and send the application form and all necessary documents to the CAB by auditable means. When the CAB has inspected the IO/RSS, the CAB shall record the approval inspection result in its database in order for the CAB to be able to check in the future whether an IO application has been previously inspected. Every employee of an IO/RSS shall be registered at the same CAB. Non approval of the IO/RSS will be notified by the CAB to all other CABs within their respective NAB's jurisdiction.

UC IO2. IO/RSS registration at VM

(see EN/ISO 18541-1:2014, use case 1.1.)

UC IO3. IO/RSS business ceases to trade

Actor	IO, RSS
Goal	Approval database is updated by CAB.
Use Case Input	The Information about the IO/RSS and its cessation of trade or IO/RSS informs the CAB about discontinuance of business.
Use Case Output	An update of the approval database, together with the revocation of all related certificates and authorisations issued to the employees of that IO/RSS.
Brief description	The CAB receives information about the IO/RSS trade cessation. The CAB informs the TC in order to revoke all certificates and authorisations issued to the employees of that IO/RSS.

UC IO4. Security-related parts ordering

Actor	IO
Goal	Supply an ordered part to IO.
Use Case Input	Authentication of IO employee. Security-related parts order.
Use Case Output	Security-related part.
Brief description	VM's shall offer security-related parts ordering facility for authorised IO employees. Manufacturers offers an online ordering facility for security-related parts using the digital certificate to confirm the identity of the person requiring the part. Alternatively, they may require security-related parts to be obtained from authorised dealers where currently established authentication procedures are in place. Security parts are delivered by VMs or their agents/authorised dealers in a timely manner to the IOs.

UC IO5. IO/RSS receives secure token

Actor	CAB
Goal	IO/RSS legal representative receives a notification that the individual IO/RSS employee is authorised to use their digital identity.
Use Case Input	Invitation to create a digital certificate forwarded by CAB.
Use Case Output	Invitation to create a digital certificate received by IO/RSS.
Brief description	The IO/RSS receives a notification from the CAB that the respective IO/RSS employee can use their digital identity. The TC delivers a notification to the respective IO/RSS employee (see UC EM6).

UC IO6. IO record keeping requirements

Actor	IO
Goal	Auditable record of transactions kept by the IO.
Use Case Input	Documents/Information provided by the repair order.
Use Case Output	Audit trail and details of the repair job.
Brief description	The IO stores state that could be required in the event of an audit. Before issuing a repair order, the IO makes sure that the following information is gathered: 1) Identification of the customer 2) Identification of the vehicle (Vehicle in place) 3) Proof of the authority of the customer to request the work to the vehicle. See procedural requirements 6.3.5.

UC IO7. Cessation of employment of an IO/RSS employee at an IO/RSS

Actor	CAB, IO, RSS, TC
Goal	Approval/Authorisation data at CAB is kept up-to-date
Use Case Input	Information about end of contract with IO/RSS employee
Use Case Output	Updated authorisation data base and request to TC to revoke the respective digital certificate.
Brief description	The IO/RSS informs the CAB about the change of employment within three working days. The CAB informs the TC in order to update the authorisation data base and to revoke the respective digital certificate. The IO is informed of the changes.

6.5 Specification of the IO/RSS employee role

The IO/RSS employee of the approved IO/RSS who is authorised as an individual to engage in security and who is provided with the necessary hardware and electronic hardware digital certificate access to the VM RMI system to obtain security-related information and performs security-related repair and maintenance activities.

6.5.1 Responsibilities and requirements

1) IO/RSS employees shall request their CAB for authorisation.

2) IO/RSS employees shall register themselves on the vehicle manufacturer's RMI system.

3) The IO/RSS employee shall access security related RMI in accordance with EN ISO 18541:2104.

4) IO/RSS employees shall ensure that all records of security related RMI downloaded from the vehicle manufacturer RMI system shall not be stored any longer than necessary for performing the operation for which the information is needed;

5) Where applicable, IO/RSS employees shall notify their IO employer that their digital certificate is no longer required;

6) IO/RSS employees shall not share with any third party the secure software token, the digital certificate or the PIN;

7) IO/RSS employees shall be responsible for using the personal secure software token and PIN correctly;

8) IO employees shall inform their IO and their TC about any loss or misuse of their security within 24 hours of such loss or misuse;

9) IO/RSS employees shall report to the relevant authorities any request or act from other IO/RSS employees relating to security related RMI that does not constitute a legitimate business activity as referred to point 6.3 of Annex X to Regulation (EU) 2018/858.

6.5.2 Functional requirements: use cases

UC EM1. IO/RSS employee requests authorisation

Actor	CAB, IO, IO employee, RSS, RSS employee, TC
Goal	IO/RSS employee receives authorisation to work with security-related RMI.
Use Case Input	IO/RSS employee meets all requirements specified in the Appendix. IO/RSS employee fills in the application form from the CAB.
Use Case Output	Authorisation of an IO/RSS employee, so that the IO/RSS employee can receive the digital certificate to access security-related RMI.
Brief description	The IO/RSS employee receives the application form from the CAB if the IO/RSS has requested the authorisation of the respective employee. The IO/RSS employee completes the application form and sends the application form and all necessary documents to the CAB by auditable means. The CAB requests a digital certificate to the IO/RSS employee and communicate the positive inspection result to the TC in order to create an authorisation record and to issue a digital certificate for this IO/RSS employee. The CAB also keeps trace of the IO/RSS employee rejection if the inspection is not successful.

UC EM2. IO/RSS employee registration at a VM

(see EN/ISO 18541-1:2014 use cases 1.2)

Actor	IO, IO employee, RSS, RSS employee, VM
Goal	To register IO/RSS employee for use of the VM RMI system as defined by the IO/RSS.
Use Case Input	- Request from the IO/RSS to register a new IO/RSS employee. User id and password of the IO/RSS are necessary. - An IO/RSS employee's request, indicating that they are associated with an IO/RSS, and are requesting confirmation from the IO/RSS legal representative to complete registration.
Use Case Output	IO´s/RSS's employee registered as an authorised user in the VM RMI system.
Description	The VM requests the IO/RSS to confirm the validity of the IO/RSS data. The VM accepts IO´s/RSS's employee as a user and informs the user accordingly. The VM RMI system asks the user to choose a User ID and either assigns an initial password to the user or allows them to enter one that satisfies the VM´s password security requirements. The VM may charge a reasonable registration fee to the IO/RSS.

UC EM3. Employee access to security-related RMI

(see EN/ISO 18541:2014 all parts)

UC EM4. IO/RSS employee download of security software/mobile application (App) (if applicable)

Actor	IO employee, RSS employee
Goal	IO/RSS employee downloads the security software/mobile app, so that the employee can use the secure digital certificate on the personal computer described in ISO 18541-2:2014.
Use Case Input	IO/RSS employee request to TC.
Use Case Output	Certificate software/mobile app
Brief description	The employee only download and install the TC software/mobile app and use the software/mobile app from the respective TC.

UC EM5. Receipt of the MFA from the CAB/TC

Actor	CAB, IO employee, RSS employee, TC
Goal	CAB provides the invitation to the IO/RSS employee to create a digital certificate with a self-chosen PIN and MFA for the digital certificate.
Use Case Input	MFA done by TC.
Use Case Output	IO/RSS employee choose their own PIN

Brief description	The IO/RSS employee chooses a PIN with software/Mobile App supplied by the TC for this identity and stores this in a security module HSM (Hardware Security Module).

UC EM6. IO employee receives the digital certificate from TC

Actor	TC, IO employee, RSS employee
Goal	Supply the digital certificate incl. MFA process description to the IO/RSS employee.
Use Case Input	Digital certificate.
Use Case Output	IO/RSS employee receives the digital certificate incl. MFA process description from TC.
Brief description	The IO/RSS employee shall receive the digital certificate incl. MFA process description from the TC with the corresponding identity.

6.5.3 IO employee – RSS employee chain authorisation setup procedure

The RSS employee requests access to the security-related RMI to act on behalf of an IO via the chain authorisation procedure that is supplied by the TC (see UC EM7). Without the approval of the IO employee the RSS employee is not entitled to execute services that are security-related on behalf of that IO employee.
Before requesting access on the VM's website for the security-related RMI or parts purchasing, module update or key commissioning, the chain authorisation must have been setup. This chain authorisation must be initiated by the IO employee directly after receiving the IOEUID of the RSS employee.
The verification of the Authority, Customer and Vehicle remains the responsibility of the IO, as described in points 7.3.5.3 to 7.3.5.5. Also issuing the repair order will be done by the IO see point 7.3.5.6.
Without this chain authorisation the RSS is not allowed to perform any security-related services on behalf of an IO.

UC EM7. Chain authorisation

Actor	IO employee, RSS employee, TC
Goal	Setup a chain authorisation between IO employee and RSS employee
Use Case Input	IO employee is requesting assistance of an RSS employee
Use Case Output	The RSS employee is entitled to preform security related services on behalf of the IO employee
Brief description	The IO employee will send a chain request to the RSS employee to grant the RSS employee the permission to act on behalf of the IO employee during the task that is given to the RSS employee.

6.6 Role of the Trust Centre

TCs shall create the digital certificates (incl. MFA process description). The respective CAB issues the authorisation to the IO/RSS and the IO/RSS employees and send the invitation for creating the digital identity. TCs shall maintain a data base of issued digital certificates. TCs shall provide vehicle manufacturers access to an interface to verify the status of the digital certificates.

TCs shall keep the information regarding IO/RSS employees in the authorisation database for an additional period of maximum 60 months. That period shall not be longer than the remaining validity period of the approval granted to the IO/RSS where the IO/RSS employee is working.

6.6.1 Responsibilities and requirements

1) The TCs can suspend and repeal digital certificate(s) upon request from the CAB;

2) The TCs shall provide the software to use the digital certificates to the IO/RSS employees;

3) The TC service shall operate 24 hours a day, 7 days a week. This will be specified in a Service Level Agreement (SLA) signed by TC, VM, CAB and SERMI (individual SLA's Actor and TC)

6.6.2 Functional requirements: use cases

UC TC1. Trust Centre creates and delivers a digital certificate/digital identity and security credentials.

Actor	CAB, TC, IO employee, RSS employee
Goal	CAB receives notification of issued digital certificates for authorisation to IO/RSS employees.
Use Case Input	Request for creation of a digital certificate/digital identity and security credentials.
Use Case Output	A MFA for the IO/RSS employee including a digital certificate/digital identity and security credentials with a by the IO/RSS employee chosen PIN.
Brief description	The CAB sends the invitation to IO/RSS employee for the creation of a digital certificate /digital identity The TC creates the digital certificate/digital identity and security credentials by using the following procedure: 1. TC issues a digital certificate/digital identity and security credentials that associates with the MFA of the IO/RSS employee by auditable means. 2. The PIN code will be chosen by the IO/RSS employee.

UC TC2. Trust Centre assesses digital certificate's/security credential validity

Actor	IO employee, RSS employee, TC, VM
Goal	Validation of the status of a authorised digital certificate/security credential.
Use Case Input	Pseudonym from the IO/RSS employee.
Use Case Output	Status supplied by TC is the following: 0 ➔ Revoked 1 ➔ Ok
Brief description	VM asks the TC for the status of employee's authorisation using the communication defined in OAuth standard.

UC TC3. Trust Centre provision of IO/RSS employee authorisation status

Actor	IO employee, RSS employee, TC, VM
Goal	Validation of authorisation status using SOAP, Restful API, OAuth and/or OIDC.
Use Case Input	Pseudonym from the IO/RSS employee.
Use Case Output	Status replied by TC is the following: Validity IOEUID/RSSEUID IOUID/RSSUID CABUID
Brief description	VM asks for IO/RSS employees authorisation status. TC responds with the authorisation status.

UC TC4. Trust Centre suspension of issued certificates

Actor	CAB, IO, RSS, RA, VM
Goal	The authorisation of the digital certificate suspension to prevent future misuse by a certificate owner in case of a detected misuse.
Use Case Input	Triggered by an appropriate employee of the actor with e.g. serial number or by other means to identify the certificate.
Use Case Output	Suspension of certificate, status updated in accordance with UC TC2. TC sends information to the CAB. CAB sends information to IO/RSS employee, as to the reason for the digital certificate suspension.
Brief description	Appropriate employee of the respective actor this employee of a CAB sends a message to the TC by auditable means. The message contains at least: - Letterhead of the respective participant. - Serial number or other means to identify the digital certificate. - Transaction number from the respective participant, if necessary. - Reason of suspension request. The suspension is processed immediately upon receipt of the suspension request. The TC inspects the origin of the message: - TC suspends the digital certificate (updated in accordance with UC TC2). - TC informs the CAB about the suspension to initiate the complaint and appeal process in written or electronic form.

UC TC5. Trust Centre suspension of an approval of an IO/RSS

Actor	CAB, RA, TC, VM
Goal	Suspension of the authorisation of all employees for a specific IO/RSS (plus all authorisations belonging to that IO/RSS) to prevent future misuses by the employees of an IO/RSS in case of detected misuses.
Use Case Input	Requested by employee representative of an authenticated actor (i.e. with an appropriate digital certificate) e.g. an employee of a CAB who is responsible for the suspension with the IO/RSS unique identifier or other means to identify the IO/RSS.
Use Case Output	Suspended authorisation(s) updated. TC sends information to the (designated) CAB
Brief description	Authenticated employee of the respective actor sends a message to the TC by auditable means. The message contains at least: - Letterhead of the respective participant. - IO/RSS unique identifier or other means to identify the IO/RSS. - Transaction number from the respective participant, if necessary. - Reason of suspension request. The suspension is processed upon receipt of the suspension request. The TC verifies the origin of the message. TC suspends all authorisations belonging to the IO/RSS. The TC informs the CAB about the suspension to initiate the complaint and appeal process in written or electronic form.

UC TC6. Trust Centres suspends IO/RSS employee´s authorisation

Actor	CAB, IO, IO employee, RSS, RSS employee, RA, VM
Goal	Suspension of authorisation of an IO/RSS employee to prevent future misuses in case of a detected misuse.
Use Case Input	Requested by a representative of an authenticated participant.
Use Case Output	Suspension of authorisation, updated authorisation database. Suspension notification to the CAB. Information to IO/RSS employee, as to the reason for the authorisation suspension.
Brief description	Authenticated employee of the respective participant e.g. an employee of a CAB who is responsible for the suspension shall send information to the TC (using a common method). The information contains at least: - Letterhead of the respective participant. - IO/RSS unique identifier. - IO/RSS employee unique identifier. - Transaction number from the respective actor, if necessary. - Reason of suspension request. The suspension is processed immediately upon receipt of the suspension request. The TC checks the origin of the information. TC suspends an authorisation belonging to an employee. TC informs the CAB about the suspension to initiate the complaint and appeal process in written or electronic form.

UC TC7. Trust Centre revokes IO/RSS approval

Actor	CAB, TC
Goal	Approval data base is kept up to date by TC.
Use Case Input	CAB notifies the decision to revoke the IO/RSS approval.
Use Case Output	IO/RSS approval classified as revoked in database.
Brief description	The TC will update the approval data base immediately after receipt of the CAB notification of the decision to revoke a particular IO/RSS. The IO/RSS approval is classified as revoke. The digital certificates and the authorisations of all IO/RSS employees of this IO/RSS are classified as revoked in the corresponding data bases.

UC TC8. Trust Centre revokes IO/RSS employee´s authorisation

Actor	CAB, TC
Goal	Digital certificate and authorisation data bases are kept up to date.
Use Case Input	CAB notifies the decision to revoke the IO/RSS authorisation.
Use Case Output	IO´s/RSS's employee digital certificate classified as revoked. IO/RSS employee´s authorisation classified as revoked.
Brief description	The TC will update the digital certificate and the authorisation data bases after receipt of the CAB notification of the decision to revoke a particular IO/RSS employee. The digital certificate and the authorisation of the IO/RSS employees of this IO/RSS are immediately classified as revoked in the corresponding data bases.

UC TC9. Trust Centre provides an environment to test the readiness of a digital certificate and the TC provided security software

Actor	IO employee, RSS employee, TC
Goal	Confirmation to the IO/RSS employee that the digital certificate + MFA works.
Use Case Input	IO/RSS employee digital certificate + PIN and MFA.
Use Case Output	Test ok / not ok. Message with failure details in case of not ok.
Brief description	The employee connects to the website of the TC. The IO/RSS employee logs on to the TC test website with his digital certificate incl. MFA. The IO/RSS employee verifies result of test (ok/not ok.) The TC logs actions for further support process (e.g. VM).

UC TC10. TC provides an interface regarding the specifications of use case CA1

Actor	TC
Goal	TC support of standard communication interface between TC and CAB (web service).
Use Case Input	Information and known standards to develop a communication interface (web service).
Use Case Output	Communication interface between TC and CAB.
Brief description	The TC develops and runs a standard communication interface for the CAB. The CAB uses this standard communication interface. It may be used for ordering the digital certificate.

UC TC11. TC provides test users with test certificates to validate the communication (OCSP, SOAP, RESTful API, OAuth and/or OIDC)

Actor	TC, VM
Goal	The functional communication between a VM and a TC.
Use Case Input	Request to the TC interface.
Use Case Output	Test data: test users, test certificates, test authorisation data base content.
Brief description	VM requests for test data in all appropriate languages for all appropriate markets. The TC sends information (test users/test certificates) which covers all possible testing outcomes to the VM.

UC TC12. Trust Centre provision of chain authorisation status

Actor	IO employee, RSS employee, TC, VM
Goal	Validation of chain-authorisation status using SOAP, Restful API, OAuth and/or OIDC.
Use Case Input	Pseudonym from the IO employee and the RSS employee
Use Case Output	The IO certificate is temporarily linked (chained) with the RSS certificate. Chain certificate generated by TC which contains: IOEUID (RSS employee) IOEUID (IO employee) CABUID
Brief description	VM asks for IO employees (RSS employee) authorisation status TC responds with the authorisation status

6.7 Role of vehicle manufacturers

Vehicle manufacturers shall provide to all approved IOs/RSSs and authorised IO/RSS employees access to security-related repair and maintenance information. Vehicle manufacturers shall communicate with TCs to verify the authorisation and authentication status of IO/RSS employees seeking access to such information.

6.7.1 Responsibilities and requirements

1) Vehicle manufacturers shall ensure that their websites are adapted to support the access of IOs/RSSs and their IO/RSS employees to security-related RMI.

2) Vehicle manufacturers shall ensure that they download the technical specifications made available on the SERMI website;

6.7.2 Procedural requirements for vehicle manufacturers

Vehicle manufacturers shall not grant access to security related RMI, unless all of the following procedural requirements have been complied with:

1. Procedural requirements for stolen vehicles
   Vehicle manufacturers shall keep a record of all vehicles of its brand reported by the authorities as stolen.
   Vehicle manufacturers shall put in place a process that provides clear traceability and accountability and enables the relevant authorities to trace the data supplied by the vehicle manufacturer to the IO employee who was granted access to the information related to the stolen vehicle.
2. Procedural requirements for storing information
   Vehicle manufacturers shall store the following information for each access granted to security-related RMI:
   a. The Vehicle Identification Number (VIN) of the vehicle for which the information was requested;
   b. The date the request was made;
   c. The vehicle registration number of the vehicle for which the information was requested, where available;
   d. Type variant of the vehicle for which the information was requested and the version of that vehicle, where available.

   Vehicle manufacturers shall store those data for 5 years.

6.7.3 Functional requirements: use cases

UC VM1. Investigation of an IO approval

Actor	VM
Goal	To investigate if an existing approval should remain valid.
Use Case Input	VM notices possible abuse/indication of abuse.

Use Case Output	The possible abuse or indication of abuse is confirmed or rejected.
Brief description	In case of non-compliance with the criteria of point 4.3.3 of Appendix 3 of Annex X to Regulation (EU) 2018/858 or with the concept of legitimate business activity set out in the second paragraph of point 6.3. of Annex X to Regulation (EU) 2018/858, the VM reports this non-compliance of an IO/RSS to the CAB. The VM starts the complaint process by informing the respective CAB. The VM is free to notify the relevant authorities, if applicable.

UC VM2. Investigation of an IO employee authorisation

Actor	VM
Goal	To investigate if existing authorisation should remain valid.
Use Case Input	VM notices possible abuse/indication of abuse.
Use Case Output	The possible abuse or indication of abuse is confirmed or rejected.
Brief description	In case of non-compliance the criteria of point 4.3.4 of Appendix 3 of Annex X to Regulation (EU) 2018/858 or with the legitimate business activity criteria set out in the second paragraph of point 6.3. of Annex X to Regulation (EU) 2018/858, the VM reports these indications of abuse to the CAB. Pending the decision of the CAB the VM may where necessarily block the IO employee internally. The VM starts the complaint process by informing the respective CAB. The VM is free to notify the relevant authorities.

UC VM3. VM blocks IOs access

Actor	VM, CAB
Goal	IO (and all connected IO employees) is denied access to security-related information.
Use Case Input	VM registers IO non-compliance regarding the terms and conditions.
Use Case Output	Access to security information blocked for the IO (and all the IO employees).
Brief description	Following its investigation, the CAB has determined that the approval should be revoked. The VM can subsequently block the IO access internally. The VM blocks the access to security information for that IO.

UC VM4. VM blocks IO employee's access

Actor	VM, CAB
Goal	VM shall have the opportunity to block an IO employee from access to security-related RMI.
Use Case Input	VM registers reason to block IO employee.
Use Case Output	Access to security information blocked for the IO employee.
Brief description	Following its investigation, the CAB has determined that the approval should be revoked. The VM can subsequently block the employee access internally. The VM blocks the access to security information for that IO employee.

UC VM5. VM verifies authorisation status of an IO/RSS employee

Actor	TC, VM
Goal	VM verifies the authorisation status when the IO/RSS employee uses the certificate for authentication to access security-related RMI.
Use Case Input	Content information of the IO/RSS employee digital certificate.
Use Case Output	Authorisation status
Brief description	The VM verifies the validity of the digital certificate (TC, OCSP, Oauth or OIDC.) The VM verifies if the IO employee is blocked (VM internal). The VM verifies the validity of the IO/RSS employee authorisation: - The VM contacts the TC by using the content information of the IO/RSS employee digital certificate. - The TC replies with the current authentication status.

UC VM6. VM download of implementation guide from SERMI website (currently OCSP, SOAP, Restful API)

Actor	VM
Goal	Compliant inspection IO/RSS employee granted an authorisation digital certificate.
Use Case Input	Request for implementation guide.
Use Case Output	Downloaded implementation guide.
Brief description	Download of implementation guide from the SERMI website. The VM inspects the IO/RSS employee digital certificate and authorisation by using the implementation guide (OCSP, SOAP/RESTful API).

UC VM7. VM supplies information to local authorities

Actor	Customer, VM
Goal	Supplying information to RA.
Use Case Input	Customer contacts local authorities. Inquiry by relevant authorities via manual process (no additional IT service required).
Use Case Output	Information about vehicle (e.g. history of actions performed on a specific VIN).
Brief description	Customer reports an offence punishable by national laws. Gives VIN or transaction information. The competent authority contacts the specific VM with an inquiry regarding a specific VIN. In the case of a stolen vehicle, if the stolen vehicle is recovered, the RA informs the VM and the status of the vehicle is restored to normal (audit trail contains information about event).

7 Technical requirements

7.1 Secure communication requirements

Any digital communication or transfer of identification, approval and authorisation data among CAB, TC and VM shall be by secure means i.e. using https-ssl/tls and mutual authentication based on X.509 certificates.

7.2 Data management description

In the SERMI-scheme only the CAB is collecting and using personal information: The following diagram describes a minimal set of attributes that are to be stored in each entity information system in order to be able to implement defined processes and use cases.

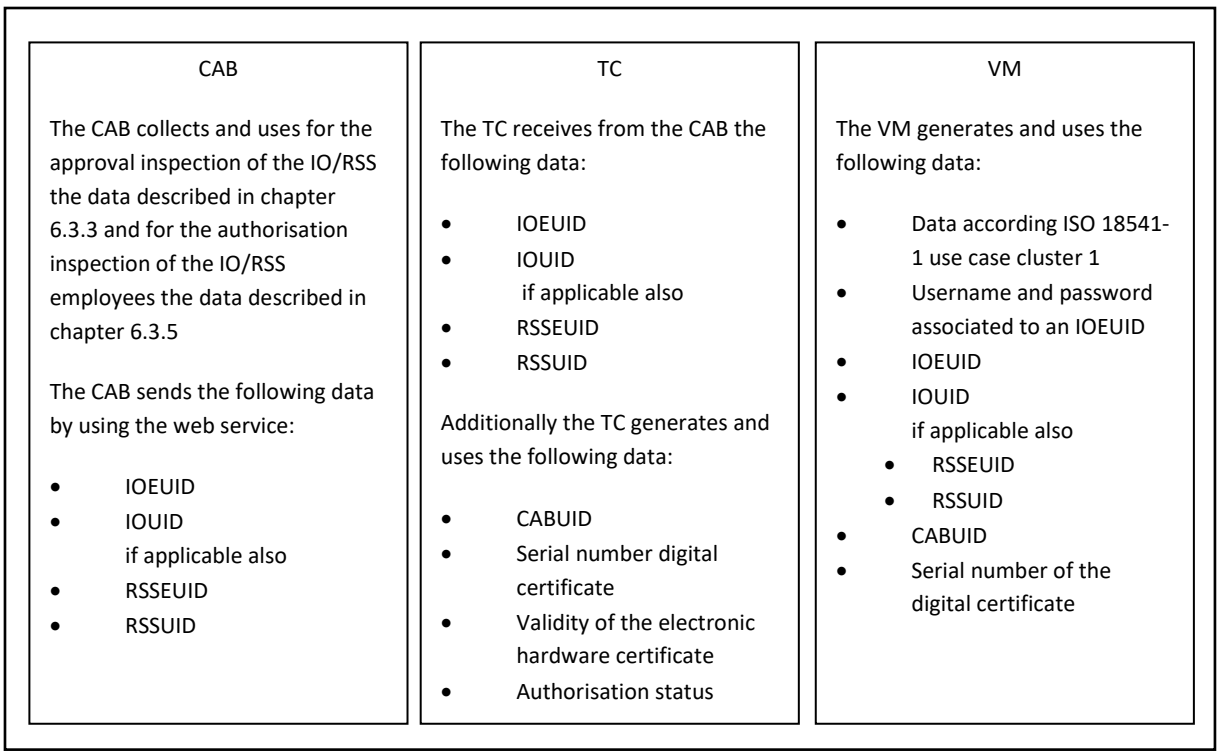

Figure 10: Example of data storage as per ISO 18541-1:2014 Use Case Cluster 1

Attribute description

1) IO employee unique identifier (IOEUID):
The identification value generated by the CAB that strictly identifies the IO employee.

2) IO unique identifier (IOUID):
The identification value generated by the CAB that strictly identifies the IO as a legal entity.

3) RSS employee unique identifier (RSSEUID):
The identification value generated by the CAB that strictly identifies the RSS employee.

4) RSS unique identifier (RSSUID):
The identification value generated by the CAB that strictly identifies the RSS as a legal entity.

5) CAB unique identifier (UID):
The identification value generated by the Trust Centre that strictly identifies the CAB.

6) Serial Number:
Contains the X509 certificate serial number, which is unique for each certificate and automatically generated during the certificate issuance.

Authorisation X / Status Authorisation X:
Describe the authorisation(s) and the corresponding status for a user.

7.3 Certificate design

The x509.V3-certificate standard (RFC 5280 and ISO 9594-8.2017) defines a list of common fields and values that shall be filled in an digital certificate.

The digital certificate is to fulfil the security requirements of the BSI (http://www.bsi.de) regarding to key length and cryptography algorithms. The point in time to apply the BSI requirements must be established by the Forum Secure RMI.

When connecting to a server using a digital certificate, the server checks a standard field named 'Subject DN' allowing it to do a link with the identity of the IO in the internal VM system.

The following figure demonstrates an excerpt of content fields, required for identification by a VM system. The complete x509.V3-certificate structure defined in the RFC 5280 is not depicted here. When using the OAuth solution, this certificate information will not be available nor required by the VM

Field	Value	Comments
Serial Number	XXX	Certificate serial number.
Issuer	XXX	Friendly name of the TC.
Validity	X years (From/To date)	Certificate lifetime from the certificate issuance to its end of validity.
Subject DN	IOEUID=<UserUniqueIdentifier>, IOUID=<IOUniqueIdentifier>, CABUID=<CABUniqueIdentifier>,	Information checked by the VM system after authentication step for identifying the user.
Subject Public Key Info	RSA encryption 4096 bits	Algorithm and value of the public key contained in the certificate.
Authority Info Access	http://XXX	OCSP server location which will be defined by the TC.

Figure 11: Content fields of the digital certificate

Validity

Validity period as defined in this scheme. Each digital certificate shall be valid for a maximum period of 60 months. This period cannot be longer than the remaining validity period of the employing IO/RSS approval.

Subject Distinguished Name (DN)

1) IOEUID / RSSEUID:
Contains a value generated by the CAB or by the TC when using an OAuth solution, which represents the IO/RSS employee identity. This value shall be unique to an authorised user: if a user requests a new digital certificate from the same CAB or another CAB (after a renewal or a revocation), he/she has to be associated to the same UID.

The IOEUID/RSSEUID is built as follows: < ISO-3166-1-COUNTRY-CODE OF THE LOCATION OF THE CAB/NAME OF THE CAB/CHARACTER ALPHANUMERIC CODE>

Example: BE/CAB-CERT/1234567890A

This value shall have a maximum of 64bits.

When using the OAuth solution, the IOEUID/RSSEUID will be generated by the TC based upon supplied information from CAB

2) IOUID / RSSUID:
Contains a value generated by the CAB or by the TC when using an OAuth solution, which represents the IO/RSS legal name, the address and the VAT or unique official business identification number.

EXAMPLE: <IO LEGALNAME:JOHNS GARAGE/ADDRESS:MAINSTREET1BRUSSELS12345/VAT:BE12345678910

When using the OAuth solution, the IOUID/RSSUID will be generated by the TC based upon supplied information from CAB

3) CABUID:
Contains a value generated by the SERMI organisation which shall be unique to an accredited CAB. This value shall have a maximum of 64bits.

The CAB has the responsibility to manage unique identifiers for users. The TC has the responsibility to manage unique identifiers IO's/RSS's legal entities. SERMI has the responsibility to manage unique identifiers for CABs, which will be added/updated by the NAB via a secured website.

Subject Public Key Info

Defines the algorithm and length of the public key contained in the digital certificate. To ensure enough confidence in the strength of the algorithm, a key length of 4096 bits or higher shall be used.

Authority Info Access

The TC shall provide an OCSP access to the certificate revocation list in order to provide an automatic access to the revocation status of the certificate. The OCSP service is provided 24/7 days.

7.4 Authorisation check Web Service based on SOAP/RESTful API or OAuth

The VM system is able to check the authorisation status of the user requesting access to security information.

This check shall provide a standard SOAP XML /RESTful API service based on HTTPS protocol. Access to this service requires authentication by an digital certificate. Request at the TC server shall be based on the following information:

Input data		
Field	Value	Comments
IO Employee Unique Identifier (IOEUID)	<IOUserUniqueIdentifier>	
RSS Employee Unique Identifier (RSSEUID)	<RSSUserUniqueIdentifier>	Only applicable if chain authorisation is used
IO Unique Identifier (IOUID)	<IOUniqueIdentifier>	
RSS Unique Identifier (RSSUID)	<RSSUniqueIdentifier>	Only applicable if chain authorisation is used
Authorisation ID	<AuthorisationUniqueIdentifier>	

Figure 12: Input data based on SOAP/RESTful API

Output data		
Field	Value	Comments
User Status	1 ➔ Ok 2 ➔ Revoked	
IO employee Unique Identifier	<IOUserUniqueIdentifier>	
RSS employee Unique Identifier	<RSSUserUniqueIdentifier>	Only applicable if chain authorisation is used

Figure 13: Output data user information details retrieval during registration based on SOAP/RESTful API

This check provides a standard SOAP XML/RESTful API service based on HTTPS protocol.