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

SERMI operations group

May 2016

Table of contents

1 Scope

This scheme is the basis for accreditation, approval and authorization of IOs requiring access to security-related vehicle RMI and services.

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

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

- Regulation (EC) No. 715/2007
- Regulation (EC) No. 692/2008 as amended by (EU) 566/2011

For heavy duty vehicles (Euro VI):

- Regulation (EC) No. 595/2009
- Regulation (EU) No. 582/2011, amended by regulation (EU) 64/2012

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 17011:2004, *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*

Directive 1999/93/EC *of the European Parliament and of the Council on a Community framework for electronic signatures*

ETSI TS 102 042, *Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates*

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 harmonized standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity.

NOTE Adopted from Regulation (EC) 765/2008

3.1.2 Approval

process based on the inspection performed by the CAB that assesses an IO company constitutes a legitimate commercial enterprise to engage in security activities and it and their individual employees comply with the requirements specified in this document.

3.1.3 Authorization

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

3.1.4 Digital certificate

digital certificate using a digital signature of the issuing Trust Center to bind a public key to the identity of the IO employee according to the standard ISO 20828. The digital certificate shall be stored in a secure hardware token with access and copy protection. The identifier is created by the CAB and the physical person's identity is only known to the CAB.

3.1.5 Secure hardware token

card or USB device protected by a PIN against unauthorized access or copy.

3.1.6 Certification database

database held by the respective Trust Center to manage the digital certificate validity and the identifiers of authorized IO employees.

3.1.7 Security-related repair and maintenance information

the required information, software, functions and services 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.

Repair and maintenance of security-related features includes:

a. updating a functionally coherent software when that software performs functions to prevent the vehicle from being stolen or driven away

b. purchasing parts that prevent the vehicle from being stolen or towed away or that could be used by unauthorised persons to give the vehicle a new identity.

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.

3.1.8 Authorization database

database held by the respective Trust Center containing the authorization details of the anonymised authorized IO employees.

3.1.9 The European co-operation for Accreditation (EA)

the body recognized by the European Commission according to article 14 in Regulation (EC)765/2008

3.1.10 The National Accreditation Body (NAB)

the single body appointed in each member state according to Regulation (EC) 765/2008

3.1.11 The Conformity Assessment Body (CAB)

The body responsible for inspection of IOs and their respective IO employees and for issuing the inspection certificates according to this scheme, so that IOs and their respective IO employees can be approved and authorized 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 authorization 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.

3.1.12 Independent Operator (IO)

IO company according to the definition given in Regulation (EC) 715/2007 that submits an application to the CAB for approval to engage employees in security-related repair and maintenance information.

3.1.13 IO legal representative

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

3.1.14 IO employee

the employee of the approved IO who is authorized as an individual to engage in security-related repair and maintenance information (RMI) access and who is provided by the CAB with the necessary secure hardware token and digital certificate.

3.1.15 Vehicle Manufacturer (VM)

vehicle manufacturer as defined in Regulation (EC) 715/2007 and whose responsibility within the scheme is to provide access to security-related RMI and functions to all authorized IO employees and who communicates with the Trust Center to verify the pseudonymised identity and authorization status of the IO employee seeking access.

3.1.16 Trust Center (TC)

body responsible for managing the digital certificates and authorization status of the IO employees and for providing to the CAB the necessary secure hardware tokens for authorized IO employees. The TC is also responsible for providing the VM with information regarding the current status of an employee´s certificate and authorization.

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

the scheme owner responsible for the definition, operation and maintenance of the accreditation scheme. This responsibility is addressed in the EA rules as scheme ownership. The members of the SERMI shall represent the stakeholders in the process for access to security-related vehicle RMI.

3.1.18 Relevant Authorities (RA)

public authorities with 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
AFCAR	Alliance for the Freedom of Car Repair in the EU
CAB	Conformity Assessment Body
CABUID	Conformity Assessment Body unique identifier
CIRCA	Communication & Information Resource Center Administrator
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
HW	Hardware
IO	Independent Operator
IOEUID	Independent Operator Employee Unique Identifier
IOUID	Independent Operator Unique Identifier
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
SOAP	Simple Object Access Protocol (Authorization Web Service)
TC	Trust Center
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 access to security-related RMI consists of two processes. One process is designed to provide the IO and its employees with an approval and authorization for access. The other process depicts the access to security-related RMI in a VM RMI system.

5.1 Approval and authorization of IO

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 the NABs in their member states.

The IO must apply for approval and employee authorization inspection to a CAB accredited in the state where the employee resides. Once the inspections for IO approval and for an individual IO employee authorization are performed with a positive result, the CAB informs the TC. The TC creates an authorization record and issues a secure hardware token and a digital certificate containing details that will allow the IO employee to be uniquely identifiable to the VM RMI website. The secure hardware token with the digital certificate is provided to the individual IO employee via the CAB. Registration of the IO employee for access to the VM RMI website and payment by the IO in 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, 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.

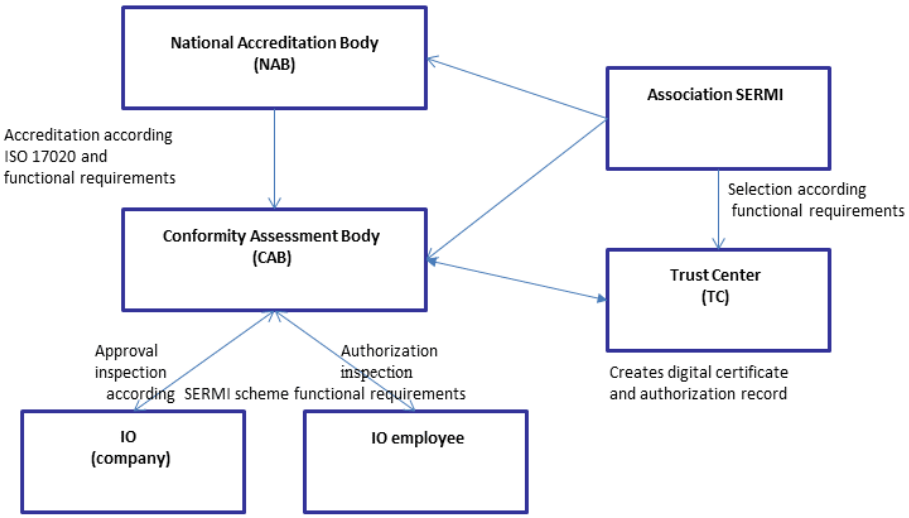

Figure 1: The bodies involved in the scheme and their relationships

The following figure describes the IO approval and IO employee authorization process.

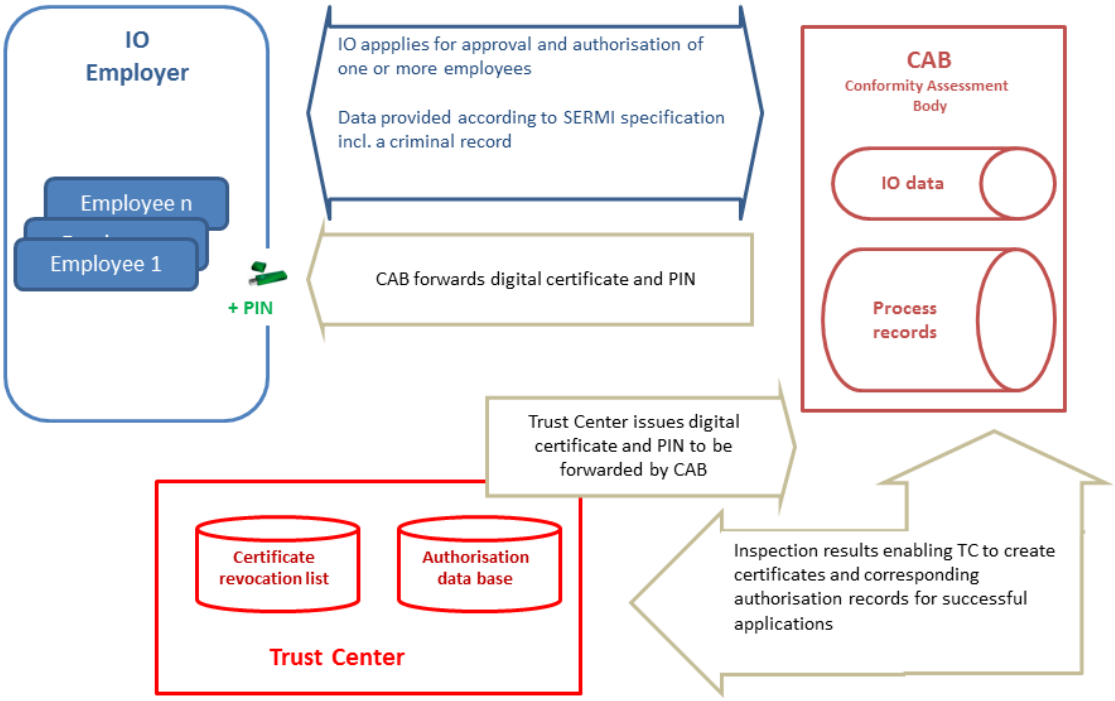

Figure 2: IO approval and IO employee authorization process

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 employee is authorized and the IO on whose behalf he is working is approved by the appropriate CAB.

Manufacturers may offer an on-line ordering facility for security-related parts using a specialized application linked to the RMI website, requiring that the IO employee is authorized and the IO on whose behalf he is working is approved by the appropriate CAB. Alternatively, security-related parts may be obtained from agents/authorized dealers 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/authorized dealers in a timely manner to the IOs.

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

An authorized and registered IO 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 employee unique identifier and appropriate authentication and authorization. Appropriate authentication of the IO employee will be done exclusively using the digital certificate. Upon receipt of the digital

certificate, the VM RMI website will verify the IO employee unique identifier and the current status of the certificate and authorization, by communicating with the appropriate Trust Center identified in the certificate.

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

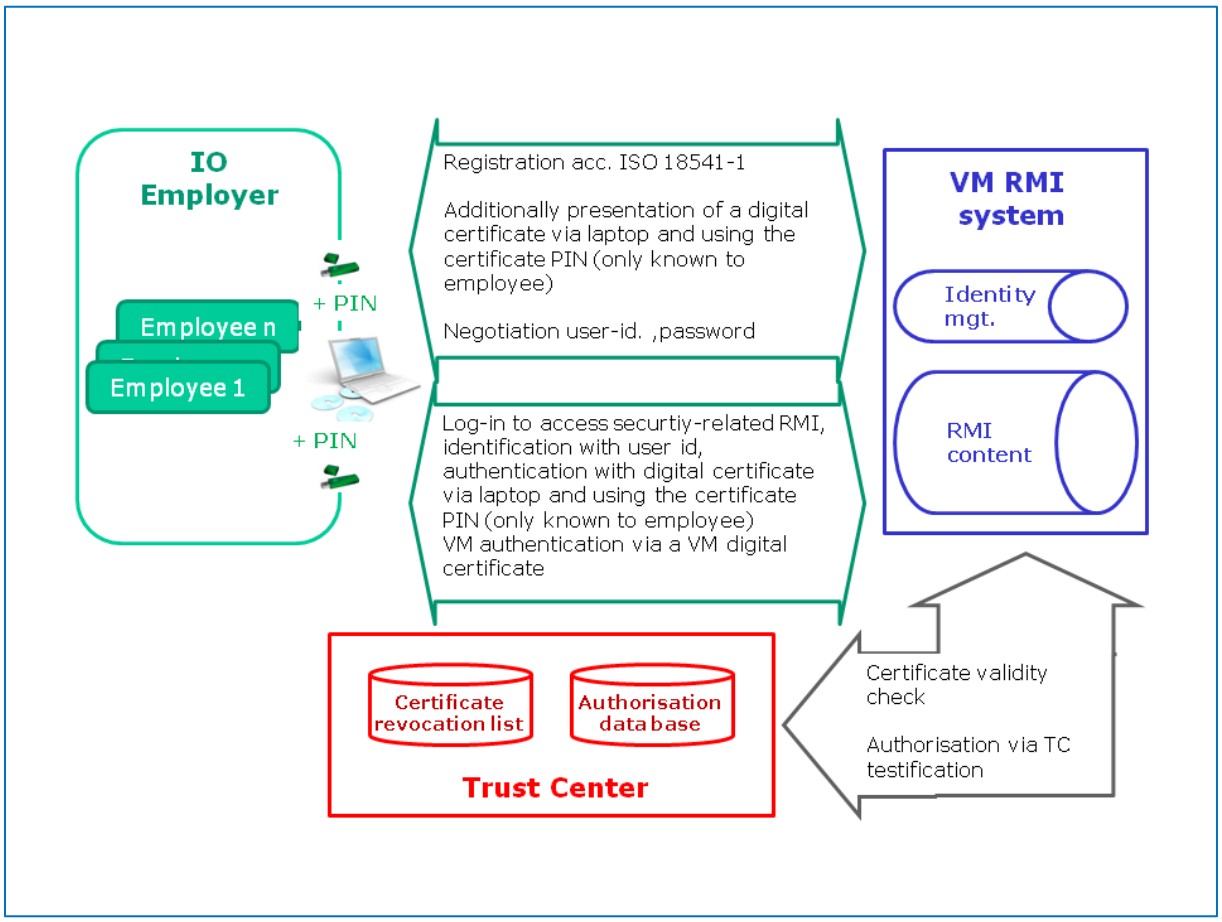

Figure 3: Access to security-related RMI

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 Center (TC) selection process.

6.1.1 Responsibilities and requirements

1) SERMI shall deal with requests for changes to the accreditation process and shall monitor the harmonization of national implementations across member states.

2) SERMI shall create the TC selection criteria and select the TC(s).

3) SERMI shall be responsible for setting the technical implementation guidelines for interaction between entities in the process.

4) SERMI shall follow the EA's norms and guidelines for scheme owners.

6.1.2 Functional requirements: use cases

UC SE1. SERMI shall deal with requests for scheme change and shall monitor the harmonization of national implementations across member states

Actor	AFCAR, ACEA, CAB
Goal	Actors may make (with good reason) 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 shall handle requests for scheme changes. Its members shall evaluate and update the scheme.

UC SE2. SERMI shall select the Trust Center (TC)

Actor	TC
Goal	To enable and appoint TC.
Use Case Input	TC´s application to SERMI which shall assess that the TC fulfills all functional and technical requirements.
Use Case Output	Accepted or rejected TC application. Updated selected TC list.
Brief description	SERMI shall process requests from TCs applying for selection according to the criteria in section 6.1.3. SERMI shall create and update the selected TC list.

UC SE3. SERMI shall be responsible for setting the implementation guide for interaction between entities in the process (e.g. using OCSP, SOAP ...)

Actor	SERMI
Goal	VMs and TC shall use the implementation guide to achieve correct implementation of the required communication standards (OCSP and SOAP).
Use Case Input	Information and known standards.
Use Case Output	Implementation guide providing all required information for the communication interfaces.
Brief description	SERMI will create and maintain the implementation considering enhancing security requirements and improving technologies over time.

6.1.3 Trust center selection

The TC will be selected by the scheme owner SERMI.

The selected TC shall comply with the standard ETSI TS 102 042, fulfill the requirements deriving from Directive 1999/93/EC "qualified electronic signature" and the requirements described in chapter 6.6.

In addition the TC shall meet the criteria outlined below:

- The technical merit of the proposal
- The capability of the Trust Center to fulfill the requirements including: technical and management competence, financial viability and relevant experience, with proven track record
- The relevant skills, experience and availability of key personnel
- Capacity of the Trust Center to operate across the European stage (EU 28)
- The existence of a quality assurance process 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 defined in Regulation (EC) 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 shall be completed by the organization applying to be a CAB. The NAB shall assess that the organization fulfills all requirements specified. The accreditation procedure shall ensure that the CAB is assessed to "Conformity assessment – Requirements for the operation of various types of bodies performing inspection" (ISO/IEC 17020) as inspection body type A, and the additional criteria described in section 6.2.3. The CAB shall request accreditation according to the rules in article 7 in Regulation (EC) No 765/2008.

UC NA2. Processing of complaints against CABs

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	It is generally expected that 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 such cases, the NAB shall deal with complaints following established procedures according to ISO 17011:2004, sec. 5.9. The accreditation body a) shall decide on the validity of the complaint, b) shall, where appropriate, ensure that a complaint concerning an accredited CAB is first addressed by the CAB, c) shall take appropriate actions and assess their effectiveness, d) shall record all complaints and actions taken, and e) shall respond to the complainant. During the complaint process through the NAB, all existing IO approvals (paper certificates) and all employee authorizations (digital certificates) than have been issued by this CAB remain valid. In case the NAB decides to withdraw the CAB accreditation all IO approvals (paper certificates) and all employee authorizations (digital certificates) than have been issued by this CAB shall be required to be renewed. SERMI shall be informed about this decision by the NAB. The CAB shall then immediately inform the approved IO about this decision by a so called end of sale notification. In case where one of the actors believes the source of the complaint has to do with the scheme definition, this shall be referred to the scheme owner SERMI according to use case SE1.

UC NA3. NAB listing of accredited CABs

Actor	NAB
Goal	NAB shall maintain an updated list of all accredited CABs.
Use Case Input	Accredited CABs.
Use Case Output	A country-specific list of accredited CABs for this country
Brief description	NAB shall create, maintain and publish a country-specific list of all accredited CABs.

6.2.3 Criteria for CAB accreditation

The CAB shall be accredited as a type A inspection body in accordance with ISO/IEC 17020. 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 inspections shall have a level of knowledge 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 approving IO commercial enterprises and authorising associated IO employees to engage in accessing security-related vehicle repair and maintenance information.

6.3.1 Responsibilities and requirements

1) The CAB shall establish a secure communication channel between the CAB and TC.

2) The CAB shall accept or reject inspection applications from IO legal representatives and IO employees from the member states by whose NAB it has been accredited.

3) The CAB shall assess applications for approval from appropriate IO legal representatives and issue an inspection certificate to IO legal representatives fulfilling the approval criteria so the TC can keep them in the Authorization database for a period of 60 months or reject applications not fulfilling the approval criteria.

4) The CAB shall notify IOs 6 months before approval expires.

5) The CAB shall assess applications for renewal of an approval where appropriate and issue a new inspection certificate for IOs fulfilling the approval criteria so the TC can keep them in the authorization database for an additional period of 60 months.

6) The CAB shall maintain the IO data relating to certification.

7) The CAB shall communicate inspection results to the TC so that IO approvals are revoked where appropriate.

8) The CAB shall assess applications for the authorization of appropriate IO employees and issue an inspection certificate to IO employees fulfilling the authorization criteria so the TC can keep them in the Authorization database for a maximum period of 60 months. This period cannot be longer than the remaining validity period of the respective IO approval.

9) The CAB shall notify IO employees 6 months before authorization expires.

10) The CAB shall assess applications for renewal of an authorization where appropriate and issue an inspection certificate to IO employees fulfilling the authorization criteria so the TC can keep them in the authorization database for an additional period of maximum 60 months. This period cannot be longer than the remaining validity period of the respective IO approval.

11) The CAB shall maintain IO employee data relating to authorizations.

12) The CAB shall shall issue a negative inspection certificate so the TC can revoke the authorization of an IO employee where appropriate.

13) The CAB shall investigate claims of misuse and assess whether authorization and approval should be revoked.

14) The CAB shall act as an interface to all IOs approved by that CAB for applications and complaints.

15) The CAB shall only collect and use data required for the approval/authorization process herein defined.

16) CAB shall deal with IO data confidentially.

17) The CAB shall communicate inspection results to the TC in order to issue the necessary secure hardware token with a digital certificate for authorized IO employees.

18) The CAB shall provide appropriate statistics to the scheme owner SERMI.

19) The CAB will only establish a business relationship with the initially selected TC for all member states.

20) In future the CAB shall only establish a relationship with TCs certified by the scheme owner.

21) The CAB shall retain secure records of approval and authorization inspections for a period of 5 years and in accordance with the law regarding data protection.

22) The CAB shall inform all other CABs in its member state about negative inspection results of an IO.

23) The CAB shall be responsible, that the data supplied during authorization and approval inspections is consistent with the requirements, e.g. ensuring that all data is identical with the original documentation.

24) The CAB shall be liable, if the data supplied by an authorized employee is not consistent with requirements for authorization inspections, e.g. copies and values are not the same.

25) The CAB shall make random und unannounced on-site checks of IOs within the 60 months approval validity period. Every approved IO shall be subjected to at least one random, on-site check over the 60 months approval validity period. A negative inspection result shall result in a revocation of the IO approval and of the IO employee authorisations.

26) The CAB shall, at the earliest make an on-site check upon IO request, 6 months prior to the validity deadline. A positive inspection result is required for the renewal of an approval.

6.3.2 Functional requirements: use cases

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

Actor	CAB
Goal	CAB shall establish a business relationship with a selected TC as published in the SERMI selected TC list.
Use Case Input	Contact with selected TC out of list of accepted TCs published by SERMI.
Use Case Output	A signed contract between CAB and TC shall be produced.
Brief description	CAB shall have a business relationship with one selected TC according to the published SERMI list (see UC SE2) in order to: a) Create digital certificates and authorization records. b) Maintain approval and authorization status (send out "new" certificate if necessary). c) Send the digital certificate and the PIN letter to be forwarded to the IO employee by the CAB. A CAB shall only set up a business relationship with one TC.

UC CA2. CAB inspects IO for approval

Actor	IO
Goal	Approval of IO, so that an IO can name employee(s) for authorization to be given access to security-related RMI.
Use Case Input	Completed application form as required by the CAB. The application form shall at least contain the criteria listed in Chapter 6.3.3.
Use Case Output	Paper certificate with the IO approval inspection result.
Brief description	IO legal representative shall send the application form and all necessary documents to the CAB by auditable means. CAB shall check the documents and check if the IO has already been inspected by another CAB. If the criteria for IO approval (see 6.3.3) are met the CAB shall send the paper inspection certificate to the IO legal representative. The CAB shall notify by auditable means the other CABs in the respective country if the IO does not pass the CAB check. CAB shall be liable for any inconsistent data. Every IO employee of an IO who becomes authorised for access to security information shall be registered at the same CAB and TC. Every approved IO shall be subjected to unannounced random checks at least once in the approval´s validity period.

UC CA3. CAB checks IO on-site

Actor	CAB
Goal	At least one random and unannounced on-site check of every approved IO during the validity period and an IO requested on-site check in the last six months of the validity period shall 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 in the application for approval.
Use Case Input	Unannounced visit to IO premises. Visit to IO premises on IO request.
Use Case Output	IO approval is confirmed or revoked. In case the IO approval is revoked, the IO employee authorizations are revoked and the TC is instructed to revoke the corresponding digital certificates.
Brief description	Qualified CAB personnel visits the IO and checks on-site the criteria in section 6.3.3 and the implementation and consideration in daily operations of the criteria in section 6.3.4. According to the findings during the check the IO approval is confirmed or revoked. The CAB may decide to allow the IO to audit ably correct minor deficiencies in a defined time period after the on-site check in order to avoid an approval revocation. A finally negative inspection result shall result in the revocation of the IO approval, the IO employee authorisations and the IO employee digital certificates by the TC.

UC CA4. CAB inspects IO for approval´s renewal

Actor	IO
Goal	Renewal of IO approval.
Use Case Input	Completed application as required by the CAB. The application form shall at least contain the criteria listed in Chapter 6.3.3. Positive result of an IO 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 approval. Expiration of IO approval, IO 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 shall be renewed. Prior to expiry of the approval the IO legal representatives shall be notified by the CAB of the pending expiry. This period of notification shall be six months before the approval ends. IO legal representative requests an on-site inspection by the CAB. The CAB performs the on-site inspection. If the inspection result is negative the CAB shall revoke the IO approval and the IO employee authorisations. The CAB instructs the TC to revoke the IO employee certificates. IO legal representative shall send all documents by auditable means to the CAB two months before the approval expires. CAB shall check the documents and check if the IO has already been approved or rejected by another CAB. If the criteria for IO approval (see 6.3.3) are met the CAB shall send the inspection paper certificate to the IO legal representatives. The CAB shall notify by auditable means, the other CABs in the respective country if the IO does not pass the CAB check. CAB shall be liable for any inconsistent data. Every employee of an IO who becomes authorized for access to security information following the authorization inspection described in use case CA6 shall be registered at the same CAB and TC.

UC CA5.CAB maintenance of IO data

Actor	IO
Goal	IO data to be correct.
Use Case Input	IO shall request the respective CAB to amend the IO data. IO legal representative shall complete the appropriate amendment form and submit it to the CAB.
Use Case Output	Updated IO data.
Brief description	IO legal representative shall send all necessary documents to the CAB by auditable means. CAB shall check the documents. If the requirements are met the CAB shall issue the paper certificate to the IO legal representatives.

UC CA6. CAB inspects IO employee for authorization

Actor	IO employee
Goal	Authorization of an IO employee or a group of IO employees.
Use Case Input	Completed inspection application form as required by the CAB. The application form shall at least contain the criteria listed in Chapter 6.3.5.
Use Case Output	Inspection result to TC in order to: 1) issue an electronic HW certificate for this IO employee, 2) create the IO employee´s authorization record in the database.
Brief description	The IO employee shall send the application and all necessary documents to the CAB by auditable means. The CAB shall check whether the IO employee had made a previous demand that had been rejected by the CAB itself or any other CAB at European level. The CAB shall check the documents. If the criteria for IO employee authorization (see 6.3.5) are met the CAB shall inform the TC in order to issue an electronic HW certificate (use case TC1). Every IO employee of an IO that seeks authorization shall be registered with the CAB and TC where the IO´s approval is registered. Pre-checking of the accuracy and completeness of information submitted by an IO legal representative on behalf of its employees is covered by ISO 17020:2012 clause 7.1.6 and section 6.3.

UC CA7. Pseudonymization of Personal Data in CAB

Actor	CAB
Goal	Pseudonymization of personal data from IO employee(s).
Use Case Input	First name, last name of the IO employee.
Use Case Output	IO employee unique identifier to be used as in the digital certificate.
Brief description	First name, last name of the IO employee is transferred to an IO employee unique identifier that will be used throughout the whole process for access to security relevant RMI. The use case ensures that the processing of personal data happens in accordance with EU-rules protecting fundamental rights and freedoms of individuals, in particular Directive 95/46/EC and Directive 2002/58/EC.

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

Actor	CAB
Goal	To provide the IO employee with a digital certificate.
Use Case Input	CAB inspection result to TC for an authorised employee.
Use Case Output	Secure hardware token with a digital certificate and a separate PIN for the IO employee sent to CAB. The IO employee shall receive the PIN associated with the digital certificate forwarded by the CAB by auditable means.
Brief description	The CAB shall send all necessary data to the TC so that the TC can produce the digital certificate, the secure hardware token and the PIN.

UC CA9. CAB inspection of an IO employee for authorization renewal

Actor	IO employee
Goal	Renewal of an employee authorization
Use Case Input	Completed inspection application form as required by the CAB. The application form shall at least contain the criteria listed in Chapter 6.3.5.
Use Case Output	Renewal inspection result of an IO employee authorization.
Brief description	The authorization shall be for a defined period after which time the authorization shall expire and will need to be renewed. The CAB shall inform the IO of the date expiry of the employees' authorization, 6 months prior to the actual date of the expiration of the authorization. IO employee shall send all documents by auditable means to the CAB 2 months before the authorization expires. The authorization inspection process described in use case CA6 shall be carried out.

UC CA10. CABs maintenance of employee's data

Actor	IO employee
Goal	The IO employee data to be correct.
Use Case Input	Request to the respective CAB to update the IO employee data. The appropriate form shall be completed and signed by the IO employee and the IO legal representative prior to submission to the CAB.
Use Case Output	Updated IO employee data.
Brief description	IO employee shall send all necessary documents to the CAB by auditable means. The CAB shall check the documents. If the update request affects the data stored in the digital certificate, the CAB shall inform the TC in order to issue a new digital certificate (use case TC1).

UC CA11. CAB procedure for complaint and appeal processes

Actor	CAB
Goal	The CAB shall have a documented process to receive, evaluate and make decisions on complaints and appeals; this process shall respect 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 has to develop and document a process for handling complaints and appeals according to EN ISO/IEC 17020:2012 (7.5). Parties wishing to make representation with regard to a perceived scheme issue shall be able to contact the respective CAB with all necessary information.

UC CA12. CAB processes a complaint concerning an IO approval

Actor	VM, TC, RA
Goal	CAB shall process complaints and appeals regarding an IO approval. IO approval shall be revoked or confirmed following the process outcome. Approval database shall be 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 approval as result of a complaint or appeal process: 1) IO approval revocation documented and IO approval classified as revoked in approval database. 2) IO employee authorizations revoked.
Brief description	The CAB investigates the complaint or appeal. 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 approval shall be revoked. In the event of a revocation the CAB shall: 1) inform the IO legal representative that the approval shall be revoked, 2) inform the respective TC in order to immediately document the approval as revoked and to revoke all digital certificates and authorizations from the IO employees of the respective IO, 3) inform all CABs in its member state about the revocation.

UC CA13. CAB processes a complaint concerning an IO employee's authorization

Actor	VM, IO, TC, RA
Goal	CAB shall process complaints and appeals regarding an IO employee´s authorization. IO employee´s authorization shall be revoked or confirmed by the TC following the process outcome. Digital certificate revocation list and authorization database shall be 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 Information of the TC in order to revoke IO employee authorization after a complaint or appeal process: 1) IO employee´s digital certificate registered as invalid. 2) IO employee's authorization status updated as invalid.
Brief description	The CAB investigates the complaint or appeal. 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 employee authorization shall be revoked. CAB shall inform the respective TC in order to immediately revoke the employee's digital certificate and the employee´s authorization. The CAB shall inform the IO legal representative about the IO employee revocation.

UC CA14. CAB provision of statistics

Actor	CAB
Goal	Monitoring of CAB.
Use Case Input	Result of approval, authorizations 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 the scheme owner SERMI (to be published on SERMI website)
Brief description	CAB analyses the results of the approval/authorization inspection process and provides a report with: • Number of investigations. • Quotient : approvals/applications • Quotient : authorizations/applications • Most common (at least 3) reasons for refusing approval • Most common (at least 3) reasons for refusing authorization • Number and outcome of on-site checks in the reporting period • Most common (at least 3) reasons for IO approval revocation • Additionally the SERMI can add other Key Performance Indicators (KPI)

6.3.3 Criteria for IO approval

The CAB shall check the following for the approval of the IO legal representative or during on-site inspection during the approval validity period.

1) Documented ownership of IO, name of managing director and legal representative.

2) Valid country specific identity card (e.g. ID card/passport) of the IO legal representative.

3) The list provided by the IO of employees who should be authorized. The check shall include information about the responsibility and the function of the employees.

4) That the IO has liability insurance. Minimum amount of coverage: 1 million Euro for bodily injury and 0.5 million Euro for property damage.

5) That the IO is not the subject of a previous revocation for reasons of misuse.

6) Proof of activity in the automotive area (e.g. membership in a relevant association, membership in a national trade organisation).

7) Legitimate business activity according to national definitions.

8) IO address.

9) The IO legal representative's name against criminal record.

10) Declaration signed by the IO legal representative that the Data Protection Regulation shall be respected.

11) Declaration signed by the IO legal representative that the compliance to the procedural requirements specified in section 6.3.4 is ensured for all operations related to vehicle security.

12) Commitment to give relevant authorities, e.g. police any information concerning a security-related operation on their request.

13) Commitment to inform the CAB when the company is dissolved or ceases to trade in the automotive business

14) Commitment to communicate immediately any changes in authorization-relevant information and circumstances of IO employees (i.e. domicile, employment relationship) to the CAB.

6.3.4 Procedural requirements for security-related operations

General behaviour

Only IO employees of the approved IO, who have been successfully authorised and are in possession of a valid electronic hardware (HW) certificate issued by the corresponding Trust Center, will access security-related RMI.

The employee shall assume personal responsibility for the correct use of the Hardware Certificate and PIN.

The IOs and their employees shall follow the procedures to deal with the end user device (PC, Laptop, etc.) as specified in ISO 18541-2 and in the annex of IO client requirements maintained by SERMI.

Procedure to conduct a security-related operation

If an employee carries out a security related software update (e.g. updating or replacing an Electronic Control Unit (ECU)) or needs other security related repair and maintenance information for a vehicle operation, the following procedure shall be followed.

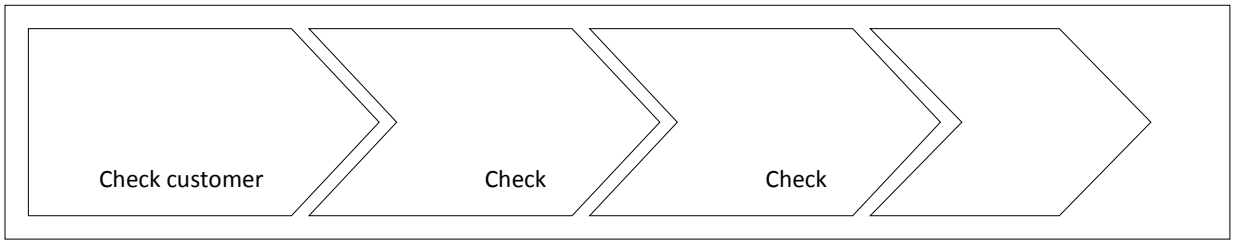

Figure 4: Basic outline of the procedure to conduct a security-related operation

Check customer

The IO employee shall check the identification of the customer, who shall be present with the vehicle.

Possible sources of identification:

➲ Identity card, passport, drivers licence, or roadside membership card

Whichever mechanism is used it shall be IOs responsibility to record the identity information in a way which can be audited.

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 5: Field reference for customer check from the vehicle registration certificate

- Name and surname of the customer
- Identity card number or number of the roadside member card

If applicable and where known the IO employee shall note the following data:

- 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 required in the circumstances where the customer will not have vehicle registration documents e.g.

1) Fleet management
2) Rental Cars
3) Loan

Check vehicle

The IO employee shall make sure that the vehicle identification number (VIN) of the vehicle is the same as the VIN on the registration documents.

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

Figure 6: Community codes from the registration documents for the vehicle check

Check authority

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.

Issue the repair order

The next step is to issue the repair order by using a dealer management system (or something similar). The repair order shall contain at least the data from figure 6 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 7: Community 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 shall be signed by the customer (owner and/or the person who brings the vehicle to the IO). The following figure describes the procedure for IO and employee.

Signed repair orders must be kept for a minimum of 5 years by the IO.

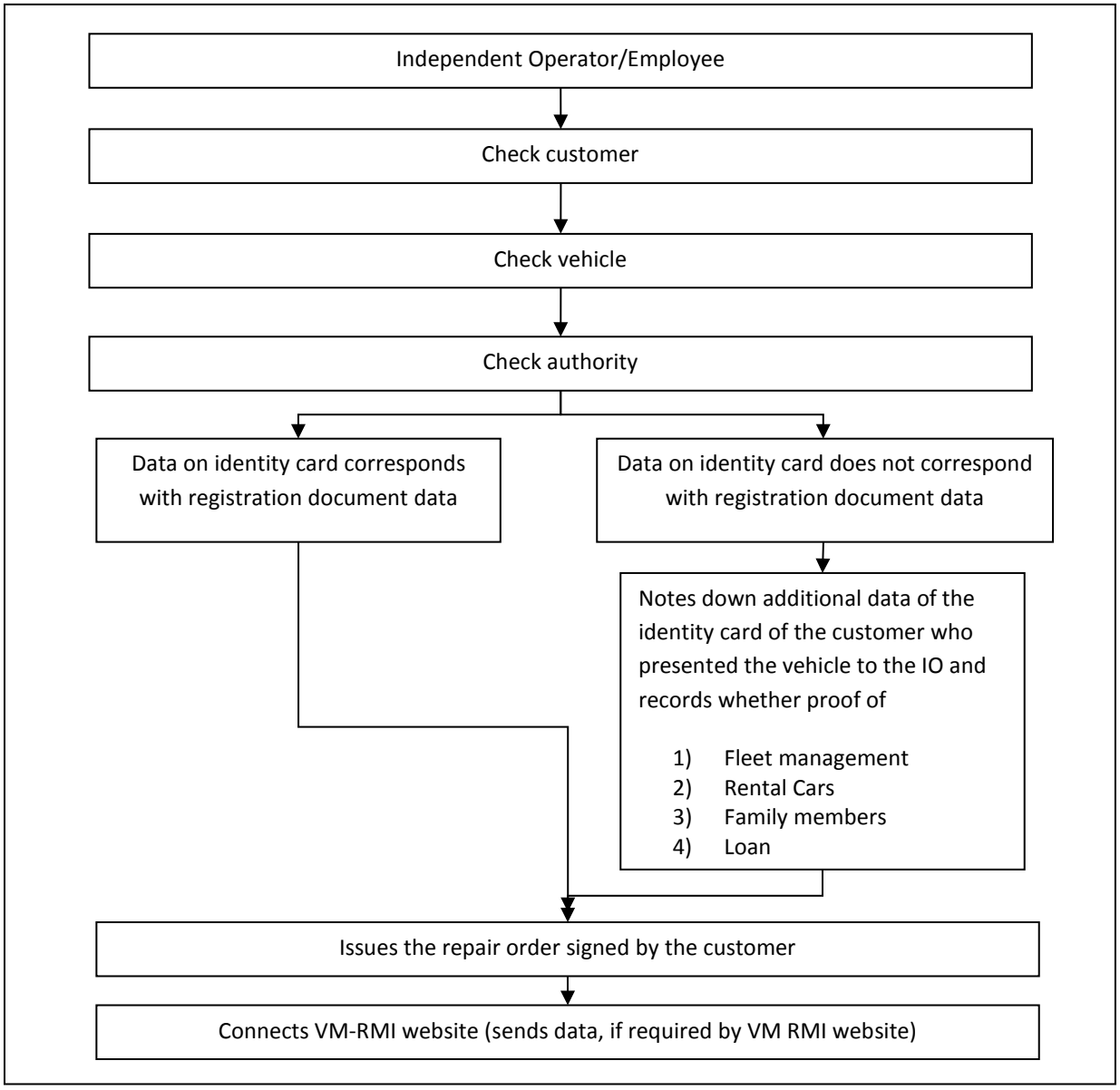

Figure 8: Procedural requirements for IO

6.3.5 Criteria for IO employee authorization

The CAB shall check the following for the authorization of the employee or during on-site inspection during the approval validity period:

1) That the employee is not the subject of a previous revocation for reasons of misuse.

2) The home address of the employee.

3) The employee's name against criminal records as prepared and presented by the IO.

4) The employment of the respective employee with the IO.

5) That the employee has signed an agreement to comply with the procedural requirements specified in section 6.3.4.

6) The approval of the IO where the employee is approved.

7) Copy (both sides) of a valid country specific identity card or equivalent (e.g. ID card/passport).

6.4 Specification of the IO role

The IO 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) The IO shall request approval inspection from the CAB.

2) The IO shall register at each VM that he/she wants to do business with.

3) The IO shall inform the CAB about changes of its data and circumstances (e.g. change of address).

4) The IO shall inform the CAB when its business is dissolved.

5) The IO shall be able to order all parts relating to security systems.

6) The IO shall use the secure hardware token supplied by the TC.

7) The IO shall maintain appropriate records for all security related RMI transactions and operations by auditable means.

8) The IO shall inform the CAB in the event of any termination of employment of an authorised employee.

9) The IO shall report any suspicion of a criminal intent or act relating to secure RMI to the relevant authorities if appropriate.

10) The IO shall ensure that the employees are correctly authorised and that the employees only use their own certificates by auditable means.

11) The IO shall ensure that the employee uses the security-related data according to the procedural requirements as specified in section 6.3.4 and especially keep record in auditable means of vehicle, customer, authority, owner and work order records.

12) The IO shall ensure that the data protection regulations are respected by all employees.

13) The IO shall also ensure that all fees relating to the employee's authorization are paid.

14) The IO shall ensure any authorized employees are appropriately trained for automotive maintenance, reprogramming and security and safety functions repair activities.

15) The IO shall request an on-site inspection by the CAB in the six months prior to the approval´s validity expiration.

6.4.2 Functional requirements: use cases

UC IO1. IO legal representative requests for approval

Actor	IO legal representative.
Goal	The IO legal representative shall meet all requirements set by the SERMI, so that the approved IO legal representative can 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 legal representative or non approval of IO legal representative.
Brief description	IO legal representative shall use the NAB website to obtain a list of accredited CAB. The IO legal representative shall contact the respective CAB. The IO legal representative shall receive the application form from the CAB. The IO legal representative shall fill 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 legal representative 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 with a negative result. Every employee of an IO legal representative shall be registered at the same CAB. Non approval of the IO will be notified by the CAB to all other CABs within their respective NAB's jurisdiction.

UC IO2. IO registration at VM

(see EN/ISO 18541-1, use case cluster 1)

UC IO3. IO business ceases to trade

Actor	IO
Goal	Approval database is updated by CAB.
Use Case Input	The Information about the IO and its cessation of trade or IO 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 authorizations issued to that IO.
Brief description	The CAB shall receive information about the IO trade cessation. The CAB shall inform the TC in order to revoke all certificates and authorizations issued to that IO.

UC IO4. 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 authorized IO employees. Manufacturers shall either offer 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 authorized dealers where currently established authentication procedures are in place. Security parts shall be delivered by VMs or their agents/authorized dealers in a timely manner to the IOs.

UC IO5. IO receives secure hardware token

Actor	CAB
Goal	IO legal representative receives secure hardware token with a digital certificate.
Use Case Input	Secure hardware token with a digital certificate forwarded by CAB.
Use Case Output	Secure hardware token with a digital certificate received by IO legal representative.
Brief description	The IO legal representative shall receive an electronic HW certificate from TC. The IO legal representative shall deliver the electronic HW certificate to the respective IO employee (see UC EM6).

UC IO6. IO record keeping requirements

Actor	IO legal representative
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 shall store legally required data, i.e. dealer management system (DMS) for audit/legal purposes. National legislation has to be taken into account. Before issuing a repair order, the IO shall make 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 6.3.4.

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

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

6.5 Specification of the IO employee role

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

6.5.1 Responsibilities and requirements

1) The IO employee shall request authorization. This shall be in conjunction with the IO.

2) The IO employee shall register on VM RMI system.

3) The IO employee shall access secure RMI according to ISO 18541.

4) The IO employee shall download software (driver for hardware to read the secure software token with the digital certificate) or be given access to the identity software by other means by the hardware provider, i.e. the Trust Center.

5) The IO employee shall receive a PIN from the TC.

6) The IO employee shall receive an electronic hardware certificate from IO legal representative.

7) The IO employee shall receive hardware to read electronic hardware certificate from IO legal representative.

8) The IO employee shall acknowledge that all records of security-related RMI downloaded from the VM RMI system may only be stored as long as it is necessary to perform the operation for which the information was needed. After the operation the data has to be definitely destroyed.

9) The IO employee shall inform his IO employer, if the digital certificate is no longer required.

10) The IO employee shall report, according to her/his IO contract, to the police of any action relating to secure RMI which is suspicious and may be criminal.

11) The IO employee shall keep the secure hardware token with the digital certificate and the PIN in a location protected against theft and shall not leave it either easily accessible to an unauthorized user.

12) The IO employee shall not pass the strictly personal secure software token with the digital certificate and/or PIN to any third party. The PIN is strictly personal and shall not be communicated to third parties in any case.

13) The employee shall be responsible for correctly using the personal secure software token and PIN.

14) The employee shall inform his IO of any changes of circumstances relating to authorization during the authorization validity period (i.e. domicile, employment relationship).

15) The employee shall inform the IO and the TC about any loss or misuse of the secure hardware token with the digital certificate within 24 hours by auditable means.

16) The IO employee is responsible for providing all authorization-relevant information and any subsequent changes (i.e. domicile, employment relationship) immediately to the CAB.

6.5.2 Functional requirements: use cases

UC EM1. IO employee requests authorization

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

UC EM2. IO employee registration at a VM

(see EN/ISO 18541-1 use cases cluster 1)

UC EM3. Employee access to security-related RMI

(see EN/ISO 18541 all parts)

UC EM4. IO employee download of software (driver for hardware to read electronic HW certificate)

Actor	IO employee
Goal	IO employee downloads the software/driver, so that he/she can use the electronic HW certificate on the personal computer described in ISO 18541-2.
Use Case Input	IO employee request to TC.
Use Case Output	Driver software
Brief description	The employee shall only download and install the TC software and use the hardware from the respective TC.

UC EM5. Receipt of the PIN from the CAB

Actor	CAB
Goal	Supply to the IO employee the PIN letter for the secure hardware token with the digital certificate.
Use Case Input	PIN from TC.
Use Case Output	PIN letter delivered to IO employee.
Brief description	The CAB prepares a PIN letter with the PIN supplied by the TC for this identity and sends it to the IO employee home address by auditable means.

UC EM6. IO employee receives the digital certificate from IO legal representative

Actor	IO legal representative, IO employee
Goal	Supply the electronic HW certificate to the IO employee.
Use Case Input	Electronic HW certificate.
Use Case Output	IO employee receives the electronic HW certificate from IO legal representative.
Brief description	The IO employee shall receive the electronic HW certificate from the IO legal representative with the corresponding identity.

6.6 Specification of the Trust Center role

The TC shall create and send the electronic hardware certificates to the IO via the respective CAB once the IO legal representative has been approved and the IO employees requesting a certificate have been authorized. The TC shall maintain a database with the validity of authorization for the IO employees. The TC shall provide an interface for use by the VM to verify the status of the certificates (via OCSP) and the status of the authorizations of IO employee's.

6.6.1 Responsibilities and requirements

1) The TC shall create and digital certificates and deliver them to IO employees via the CABs.

2) The TC shall maintain a database (OCSP) of revocations of digital certificates.

3) The TC shall maintain a database of employee's authorizations.

4) The TC shall suspend digital certificate(s) where appropriate.

5) The TC shall suspend IO employee authorizations where appropriate.

6) The TC shall provide the software to use the digital certificate(s).

7) Optional: The TC shall provide an environment to test the readiness of a certificate and the TC provided software.

8) The TC shall provide an interface with the VMs in accordance with the technical implementation guidelines from the Forum Secure RMI.

9) The TC shall provide "test users" with test certificates to validate the communication between VM and TC for requesting the status of authorization and authentication of the IOs and employees.

10) The TC shall download the test protocols from SERMI website (e.g. OCSP & SOAP).

11) The TC shall operate in accordance with the functional requirements in section 6.6.2 and technical requirements in chapter 7 of this report.

12) The TC shall operate on a 24/7 basis.

13) The TC shall support the following technologies: CSP/PKCS#11, OCSP, SOAP.

14) The TC shall be able to use "qualified electronic signature" in accordance with Directive 1999/93/EC.

15) The TC shall comply with the standard ETSI TS 102 042.

16) A TC shall establish a business relationship including the necessary interface with an accredited CAB.

17) The TC shall apply the procedures and specifications defined in the technical implementation guidelines by SERMI.

6.6.2 Functional requirements: use cases

UC TC1. Trust Center creates and delivers certificate

Actor	CAB
Goal	CAB receives certificates and PIN for distribution to IO employees
Use Case Input	Request for creation of a digital certificate.
Use Case Output	Digital certificate and PIN.
Brief description	The CAB shall contact the TC (see use case CA11 for procedure). The TC shall create the digital certificate and provide it to the CAB for distribution to the IO employee by using the following procedure: 1) TC shall send the personalized digital certificate to the CAB by auditable means. 2) The pin code shall be sent separately by auditable means separately to the CAB.

UC TC2. Trust Center assesses digital certificate's validity

Actor	VM
Goal	Validation of the status of a digital certificate.
Use Case Input	Digital certificate serial number.
Use Case Output	Status supplied by TC is the following: 0 ➔ Suspended 1 ➔ Ok 2 ➔ Revoked 3 ➔ Unknown
Brief description	VM shall ask for the status of employees digital certificate for authentication using the communication defined in OCSP standard. The TC shall respond regarding the OCSP-responder status. The TC maintains for this purpose a revocation database according to the OCSP standard.

UC TC3. Trust Center provision of IO employee authorization status

Actor	VM
Goal	Validation of authorization status using SOAP.
Use Case Input	Digital certificate serial number and attributes.
Use Case Output	Status replied by TC is the following: Validity IOEUID IOUID CABUID
Brief description	VM shall ask for IO employees authorization status. TC shall respond regarding the authorization status.

UC TC4. Trust Center suspension of issued certificates

Actor	VM, IO, CAB, RA
Goal	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 OCSP updated. TC sends information to the CAB. Information to IO employee, as to the reason for the digital certificate suspension.
Brief description	Appropriate employee of the respective participant e.g. an employee of a CAB who is responsible for the suspension sends a message to the TC by auditable means. The message shall at least contain: - Letterhead of the respective participant. - Serial number or other means to identify the certificate. - Transaction number from the respective participant, if necessary. The suspension shall be processed immediately upon receipt of the suspension request. The TC shall check the origin of the message and having confirmed the authenticity of the message: - TC shall suspend the digital certificate (updated OCSP). - TC shall inform the CAB about the suspension to initiate the complaint and appeal process in written or electronic form.

UC TC5. Trust Center suspension of an approval of an IO

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

UC TC6. Trust Centers suspends IO employee´s authorization

Actor	VM, IO, CAB, relevant authorities
Goal	Suspension of authorization of an IO employee to prevent future misuses in case of a detected misuse.
Use Case Input	Requested by a legal representative of an authenticated participant.
Use Case Output	Suspension of authorization, updated authorization database. Suspension notification to the CAB. Information to IO employee, as to the reason for the authorization 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 shall at least contain: - Letterhead of the respective participant. - IO unique identifier. - IO employee unique identifier. - Transaction number from the respective actor, if necessary. The suspension shall be processed immediately upon receipt of the suspension request. The TC shall check the origin of the information. TC shall suspend one authorization belonging to an employee. TC shall inform the CAB about the suspension to initiate the complaint and appeal process in written or electronic form.

UC TC7. Trust Centers revokes IO approval

Actor	CAB
Goal	Approval data base is kept up to date.
Use Case Input	CAB notifies the decision to revoke the IO approval.
Use Case Output	IO 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. The IO approval is classified as revoke. The digital certificates and the authorizations of all IO employees of this IO are immediately classified as revoked in the corresponding data bases.

UC TC8. Trust Centers revokes IO employee´s authorization

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

UC TC8. Trust Center provision of the software to handle a certificate (CSP and PKCS#11)

Actor	IO, IO employee (optional VM)
Goal	IO employee is operational and is able to access secure RMI.
Use Case Input	TC website is accessed to download the necessary software package and information on how to install the software.
Use Case Output	Employee shall be in an operational environment to handle the electronic HW certificate.
Brief description	The TC shall provide all necessary software to use the electronic HW certificate as well as information about the minimum system requirements. The software shall include a cryptographic service provider (CSP) for Windows operating systems (e.g. Windows 7, Windows 8.1, and Windows 10) and a Public Key Cryptography Standard#11 (PKCS#11) module for Windows.

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

Actor	IO employee
Goal	Confirmation to the IO employee that the electronic HW certificate works.
Use Case Input	IO employee electronic HW certificate + PIN and software on client PC.
Use Case Output	Test ok / not ok. Message with failure details in case of not ok.
Brief description	The employee shall connect to the website of the TC. The IO employee shall log on to the TC test website with his electronic HW certificate. The IO employee shall see result of test (ok/not ok.) The TC shall log actions for further support process (e.g. VM).
Comments	

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 shall develop and run a standard communication interface for the CAB. The CAB shall use this standard communication interface e.g. for ordering the digital certificate.

UC TC11. TC provides test users with test certificates to validate the communication (OCSP & SOAP)

Actor	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 authorization database content.
Brief description	VM request for test data in all appropriate languages for all appropriate markets. The TC shall send information (test users/test certificates) which covers all possible testing outcomes to the VM.

6.7 Specification of VM role

The vehicle manufacturer role is to provide access to security-related repair and maintenance information to all approved IOs and authorized IO employees. VMs shall communicate with the Trust Center to verify the authorization and authentication status of the IO employee seeking access.

6.7.1 Responsibilities and requirements

1) Vehicle manufacturers shall initiate an investigation of an IO approval if appropriate.

2) Vehicle manufacturers shall initiate an investigation of an employee's authorization if appropriate.

3) Vehicle manufacturers shall block an IO if appropriate.

4) Vehicle manufacturers shall block an IO employee´s access to secure RMI if appropriate.

5) Vehicle manufacturer shall request suspension of the IO approval in case of suspected abuse. All authorizations of all employees belonging to this IO shall be suspended if appropriate.

6) Vehicle manufacturer shall request suspension of the IO employee authorization in case of suspected abuse.

7) Vehicle manufacturers shall identify a legal representative who is authorized to request suspension of an IO employee authorization.

8) Vehicle manufacturers shall be allowed to check the validity of an IO employee´s digital certificate.

9) Vehicle manufacturers shall be allowed to check the authorization status of an employee.

10) Vehicle manufacturers shall download the technical specification from SERMI website.

11) Vehicle manufacturers shall provide an audit trail to relevant authorities.

12) VM has to support the agreed technologies in this report (e.g. OCSP, SOAP, PKCS#11).

6.7.2 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	If the VM notices abuse, the VM shall report this indication of abuse by an IO to the CAB (during normal office hours) and block the IO employees internally. The VM may start the complaint process by informing the respective CAB. The VM is free to notify the police, if applicable.

UC VM2. Investigation of an employee authorization

Actor	VM
Goal	To investigate if existing authorization 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	If the VM notices abuse, the VM shall report these indications of abuse to the CAB (at normal office hours) and block the IO employee internally. The VM may start the complaint process by informing the respective CAB. The VM is free to notify the police, if applicable.

UC VM3. VM blocks IO

Actor	VM
Goal	IO (and all connected IO employees) is denied access to security-related information.
Use Case Input	VM registers IO misbehavior regarding the terms and conditions.
Use Case Output	Access to security information blocked for the IO (and all the IO employees).
Brief description	The VM shall block the IO access internally. The VM shall use the same criteria to block IO as he uses to start corresponding actions in his own organisation. The VM may ask for IO approval suspension and start the complaint process by informing the respective CAB.

UC VM4. VM blocks IO employee

Actor	VM
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	The VM shall block the employee access internally. The digital certificate of the IO employee blocked by one VM remains valid. The VM shall use the same criteria to block IO employees as he uses to start corresponding actions in his own organisation. The VM may ask for IO employee authorization suspension and start the complaint process by informing the respective CAB.

UC VM5. VM checks authorization status of an employee

Actor	VM
Goal	VM shall check the authorization status when the employee uses the certificate for authentication to access security-related RMI.
Use Case Input	Content information of the employee electronic HW certificate.
Use Case Output	Authorization status
Brief description	The VM shall check the validity of the certificate (TC, OCSP.) The VM shall check if the employee is blocked (VM internal). The VM shall check the validity of the employee authorization: - The VM shall contact the TC by using the content information of the employee electronic HW certificate. - The TC shall reply with the current authentication status.

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

Actor	VM
Goal	Compliant check IO employee electronic HW certificate and authorization.
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 shall check the IO employee electronic HW certificate and authorization by using the implementation guide (OCSP, SOAP).

UC VM7. VM supplies information to local authorities

Actor	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 crime/gives VIN or transaction information. A relevant authority, such as e.g. the police contacts a specific vehicle manufacturer with an inquiry regarding a specific VIN. VM, IO return information about audit trail to the relevant authority. 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).

6.7.3 Procedural requirements for VM

Before the request for secure RMI by an IO employee is answered by the VM, the VM shall fulfil the following procedural requirements:

- Procedural requirements for stolen vehicles
- Procedural requirements for the “Audit trail”

Stolen vehicles

The VM shall keep a record of vehicles of his brands reported as stolen by authorities.

The VM shall take appropriate measures on a reported stolen vehicle in accordance with local law: e.g. communicate to authorities, deny repair, repair and report to authorities.

Audit trail

It is important to trace and remedy faults or misuse of the system in the event of a stolen vehicle using information supplied to an Independent Operator (IO).

The audit system must provide clear traceability and accountability which enables the relevant authorities to trace the data supplied by the Vehicle Manufacturer (VM) to the IO employee who uses it for the subsequently stolen vehicle.

The Vehicle Manufacturer should provide without unnecessary delay available data on request of the relevant authorities within working days. Data available showing when an IO accessed the VM-RMI website. This requirement in no way replaces existing processes and procedures currently agreed between VMs and relevant authorities.

The following information for each access to security-related repair and maintenance information shall be stored by the respective Vehicle Manufacturer.

- Vehicle Identification Number (VIN)
- Date of transaction
- Kind of information
- Certificate details, which can identify the certificate owner.
- Vehicle registration number (if possible)
- Type variant, version of the respective vehicle (if possible)

The VM shall store this data for a time period of 5 years.

Relevant authorities e.g. police shall have access to this information by contacting the respective Vehicle Manufacturer.

7 Technical requirements

7.1 Secure communication requirements

Any digital communication or transfer of identification, approval and authorization 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 doesn't describe a database implementation model but defines a minimal set of attributes that has to be stored in each entity information system in order to be able to implement defined processes and use cases.

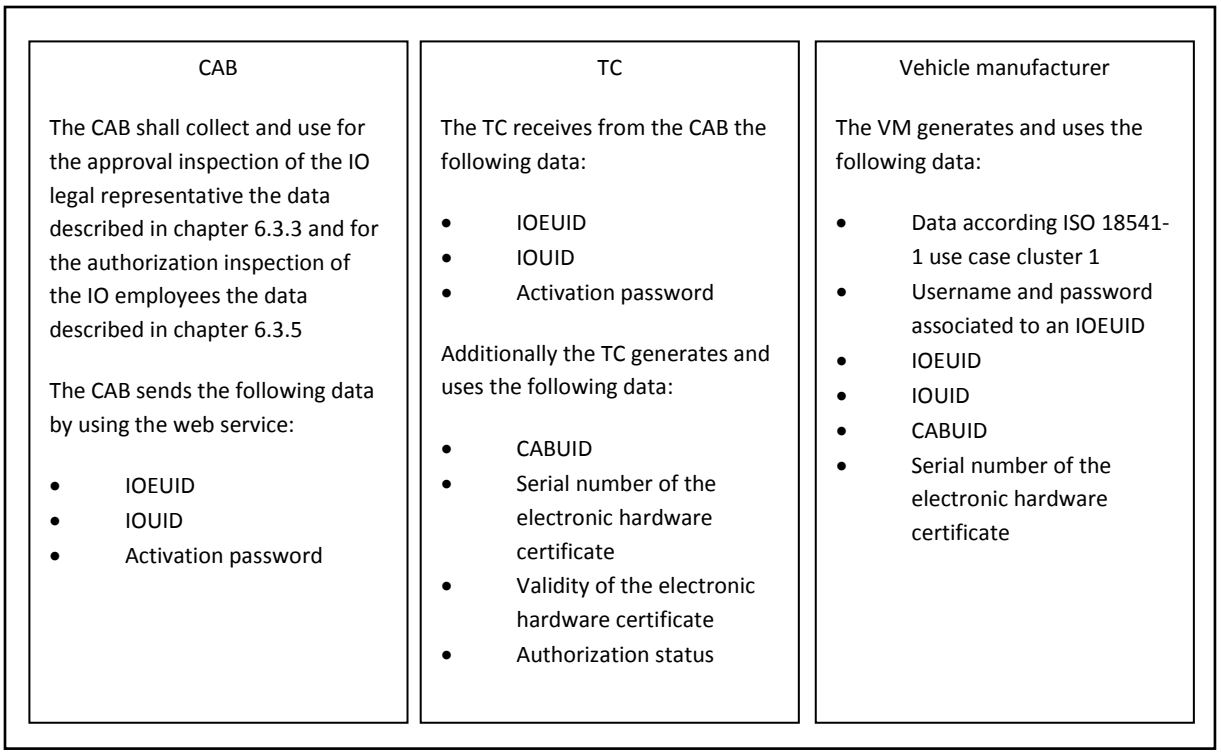

Figure 9: Example of data storage

Attribute description

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

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

3) CAB unique identifier (UID):
The value generated by the Trust Center that strictly identifies the CAB.

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

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

7.3 Certificate design

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

The digital certificate shall fulfill 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.

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 10: Content fields of the electronic hardware certificate

Validity

Validity period as defined in this scheme. Each electronic hardware certificate shall be valid for a maximum period of 36 months. This period cannot be longer than the remaining validity period of the employing IO approval.

Subject Distinguished Name (DN)

1) IOEUID:
Contains a value generated by the CAB which represents the IO employee identity. This value shall be unique to an authorised user: if a user requests a new electronic hardware 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 is built as follows: < ISO-3166-1-COUNTRY-CODE OF THE LOCATION OF THE CAB/NAME OF THE CAB/CHARACTER ALPHANUMERIC CODE>

Example: DE/NEOCERT/1234567890A

This value shall have a maximum of 64bits.

2) IOUID:
Contains a value generated by the CAB which represents the IO legal name, the address and the VAT number.

EXAMPLE: <IO LEGALNAME:NEO/ADRESS:MAINSTRASSE34BONN53129/VAT:DE12345678910

3) CABUID:
Contains a value generated by the TC 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 legal entities and CAB.

Subject Public Key Info

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

Authority Info Access

The Trust Center 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 shall provide 24/7 days.

7.4 Authorization check Web Service based on SOAP

The VM system shall be able to check the authorization status of the user requesting access to security information.

This check shall provide a standard SOAP XML service based on HTTPS protocol. Access to this service shall be authenticated by an electronic certificate. Request at the TC server shall be based on the following information:

Input data		
Field	Value	Comments
IO Employee Unique Identifier (IOEUID)	<UserUniqueIdentifier>	
IO Unique Identifier (IOUID)	<IOUniqueIdentifier>	
Authorization ID	<AuthorizationUniqueIdentifier>	

Figure 11: Input data

Output data		
Field	Value	Comments
User Status	0 ➔ Suspended 1 ➔ Ok 2 ➔ Revoked 3 ➔ Unknown	
IO employee Unique Identifier	<UserUniqueIdentifier>	

Figure 12: Output data user information details retrieval during registration based on SOAP

This check shall provide a standard SOAP XML service based on HTTPS protocol. A VM specific electronic hardware certificate shall authenticate access to this service.