EUROPEAN
COMMISSION

Brussels, XXX
[…](2020) XXX draft

ANNEX

ANNEX

to the

Commission Delegated Regulation (EU) .../...

amending Annex X to Regulation (EU) 2018/858 of the European Parliament and of the Council as regards the standardised access to vehicle on-board diagnostics information and repair and maintenance information, and the requirements and procedures for access to vehicle security information

ANNEX

Annex X to Regulation (EU) 2018/858 is amended as follows:

(1) point 2.1 is replaced by the following:

'2.1. A manufacturer shall put in place the necessary arrangements and procedures, in accordance with Article 61(2), to ensure that vehicle OBD information and vehicle repair and maintenance information is accessible through websites. Compliance with the obligation for manufacturers to provide OBD information and vehicle repair and maintenance information on their websites through a standardised format shall be presumed by conforming to Part 1 'General information and use case definition', Part 2 'Technical requirements', Part 3 'Functional user interface requirements', Part 4 'Conformance test' and Part 5 'Heavy duty specific provision' of standard ISO 18541 – 2014 'Road vehicles — Standardized access to automotive repair and maintenance information (RMI)'. Access to vehicle OBD information and vehicle repair and maintenance information shall be granted in a readily accessible and prompt manner.';

(2) point 2.5.2 is replaced by the following:

'2.5.2.service handbooks, including service and maintenance records, and technical specifications references regarding fluids including on lubricants, brake fluids and cooling liquids;';

(3) in point 2.9, the first paragraph is replaced by the following:

'For the purpose of vehicle diagnostics, repair and maintenance, monitoring and inspection, the direct vehicle data stream, including fault codes, and diagnostic functions, shall be made available through the serial data port on the standardised data link connector specified in paragraph 6.5.1.4 of Appendix 1 of Annex 11 to Regulation No 83 of the Economic Commission for Europe of the United Nations (UN/ECE)[1] and paragraph 4.7.3 of Annex 9B to Regulation No 49 of the Economic Commission for Europe of the United Nations (UN/ECE)[2]';

(4) in point 6.1., the first paragraph is replaced by the following:

'Vehicle OBD information and vehicle repair and maintenance information available through websites shall comply with the Parts of standard ISO 18541 – 2014 referred to in point 2.1.';

(5) point 6.3 is amended as follows:

(a) the first sentence is replaced by the following:

[1] Regulation No 83 of the Economic Commission for Europe of the United Nations (UN/ECE) — Uniform provisions concerning the approval of vehicles with regard to the emission of pollutants according to engine fuel requirements (OJ L 42, 15.2.2012, p. 1).

[2] Regulation No 49 of the Economic Commission for Europe of the United Nations (UN/ECE) — Uniform provisions concerning the measures to be taken against the emission of gaseous and particulate pollutants from compression-ignition engines for use in vehicles, and the emission of gaseous pollutants from positive-ignition engines fuelled with natural gas or liquefied petroleum gas for use in vehicles (OJ L 180, 8.7.2011, p. 53).

‘The procedure for the approval and authorisation of independent operators to access vehicle security features as referred to in point 6.2 is set out in Appendix 3. The role and responsibilities of the bodies involved in the accreditation, approval and authorisation of independent operators are detailed in the functional requirements consisting examples and use cases laid down in Commission Notice ….’;

(b) the following paragraph is added:

‘For the purposes of that procedure, operators shall not be considered to pursue a legitimate business activity where they advertise or offer repair or maintenance operations that would negatively impact the emissions performance of the vehicle. This shall include:

(c) deactivating or removing pollution control devices or emission control systems, or degrading their performance or concealing their malfunction;

(d) installing defeat devices[3], or defeat strategies[4];

(e) deactivating, removing or tampering[5] with devices for the monitoring of the consumption of fuel or electric energy, or tampering with odometer readings;

(f) tampering with the engine control unit, including the rated engine power.’;

(6) the following Appendix 3 is added:

‘Appendix 3

Procedure for the approval and authorisation of independent operators to access vehicle security features[6]

1. Scope

This Appendix contains the requirements for the purposes of accreditation, approval and authorisation of independent operators requiring access to security-related vehicle repair and maintenance information (RMI) services.

It specifies in detail the process and the bodies required to approve and authorise independent operators to be granted access to security-related vehicle repair and maintenance information for light passenger and commercial vehicles and heavy duty vehicles.

2. Definitions, symbols and abbreviated terms

2.1. Definitions

For the purposes of this Appendix, the following definitions shall apply:

2.1.1. 'Accreditation'

‘accreditation’ shall mean accreditation as defined in Article 2, point 10 of Regulation (EC) No 765/2008

2.1.2. 'IO employee'

[3] As defined in Article 3(10) of Regulation (EC) No 715/2007.

[4] As defined in Article 3(8) of Regulation (EC) No 595/2009.

[5] As defined in Article 3(16) of Regulation (EC) No 595/2009.

[6] The requirements set out in this Appendix are based on those laid down in the ‘Scheme for accreditation, approval and authorization to Access Security-related Repair and Maintenance Information (RMI)’ validated on 19 May 2016 by the European co-operation for Accreditation (https://www.vehiclesermi.eu/)

‘IO employee’ shall mean the employee of an approved IO who, upon authorisation from his or her CAB, will have access security-related RMI

2.1.3. 'Security-related repair and maintenance information' or 'security-related RMI'

'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 that are 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.

2.1.4. 'Approval inspection certificate'

'approval inspection certificate' shall mean the certificate issued by the CAB to IOs complying with the approval criteria set out in this Appendix and which confirms that those IOs are approved and that IO employees can request the authorisation to access security-related RMI.

2.1.5. 'Authorisation inspection certificate'

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

2.1.6. 'Trust centre' or 'TC'

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

(a) managing the digital certificates and authorisation status of the IO employees and for providing to the CAB the necessary secure hardware tokens and digital certificates for authorised IO employees;

(b) providing a vehicle manufacturer with information regarding the authorisation status of an IO employee.

2.1.7. 'Secure hardware token'

'secure hardware token’ shall mean a card or USB device protected against unauthorised access or copy by a PIN.

2.1.8. '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 employee in accordance with the standard ISO 9594.

2.1.9. 'Authorisation database'

'authorisation database’ shall mean a database held by the trust centre and which contains the authorisation details of the anonymised authorised IO employees and the registration of approved IOs.

2.1.10. 'Certification database'

‘certification database' shall mean a database held by the trust centre to manage the digital certificate validity and the identifiers of authorised IO employees.

2.1.11. 'European co-operation for Accreditation' or '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.

2.1.12. 'Forum for Access to Security-Related Vehicle RMI' or '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 .

2.1.13. 'Relevant authorities'

'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. Accreditation of CABs, approval of IOs and authorisation of IO employees

Only CABs that are accredited by the national accreditation body ('NAB'), as defined in Article 2, point 11 of Regulation (EC) No 765/2008, of the Member State in which they are established shall issue approval inspection certificates certifying that an IO has been approved and authorisation inspection certificates certifying that an IO employee is to access security-related RMI.

The approval of the IO and the authorisation of the IO employee shall be granted for a period of 60 months starting from the date of issuance of the relevant inspection certificates.

IOs wishing to receive security-related RMI shall obtain an approval inspection certificate from a CAB accredited by the NAB of the Member State where the IO is established.

IO employees who are to handle security-related RMI shall obtain an authorisation inspection certificate from a CAB accredited by the NAB of the Member State where the IO employee resides.

CABs shall inform TCs of any approval inspection certificates or authorisation inspection certificates issued, upon which TCs shall create an authorisation record and issue a secure hardware token and a digital certificate containing details that allow IO employees to be uniquely identifiable to the vehicle manufacturer RMI website. CABs shall provide individual IO employees with a secure hardware token and the digital certificate.

Vehicle manufactures may demand a fee for the registration of IO employees on those vehicle manufacturers' RMI websites and for access to security-related RMI. Such fee shall be proportionate to the cost for such registration and provision of access. The fees due shall be specified on the vehicle manufacturers' RMI websites. All digital data transfers between IOs, TCs and CABs shall be carried out via business to business (B2B) transactions using secure protocols and in a timely manner.

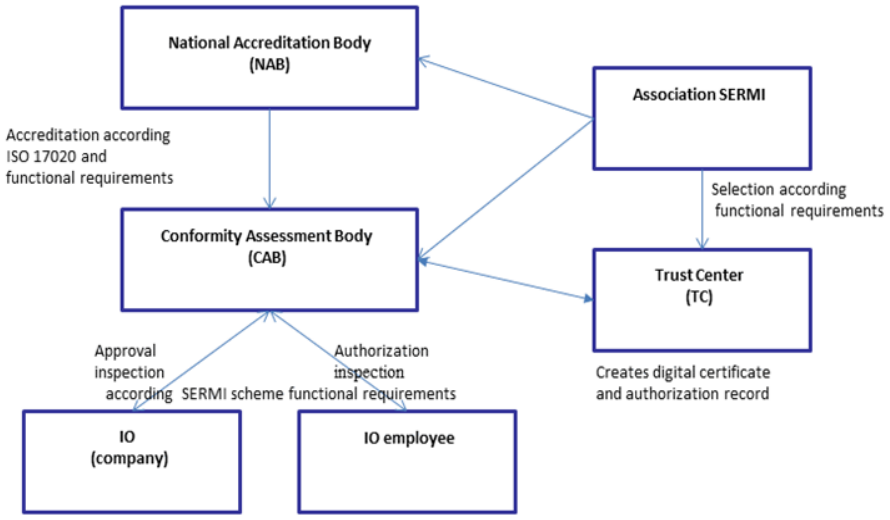

Figure 1: The bodies involved in the accreditation of CABs, approval of IOs and authorisation of IO employees and their relationship

A declaration that certifies that the IO pursues a legitimate business activity as referred to in point 6.3. of this Annex shall be signed by the IO requesting to be authorised by the CAB. An IO shall only be approved after an inspection by the CAB that shall verify that this declaration has been signed and that shall assess whether the IO and its individual employees comply with the requirements laid down in this Appendix.

Individual IO employees shall only be authorised after an inspection by a CAB.CABs shall check the documents submitted and shall verify whether the IO employee concerned made a previous request for authorisation that has been rejected by the CAB concerned or any other CAB at Union level.

CABs shall send all data to the TC that are necessary for the TC to produce the digital certificate and the secure hardware token, which the CAB shall send to the IO employees..

IO employees that have been authorised shall receive from their CABs the PIN associated with the digital certificate.

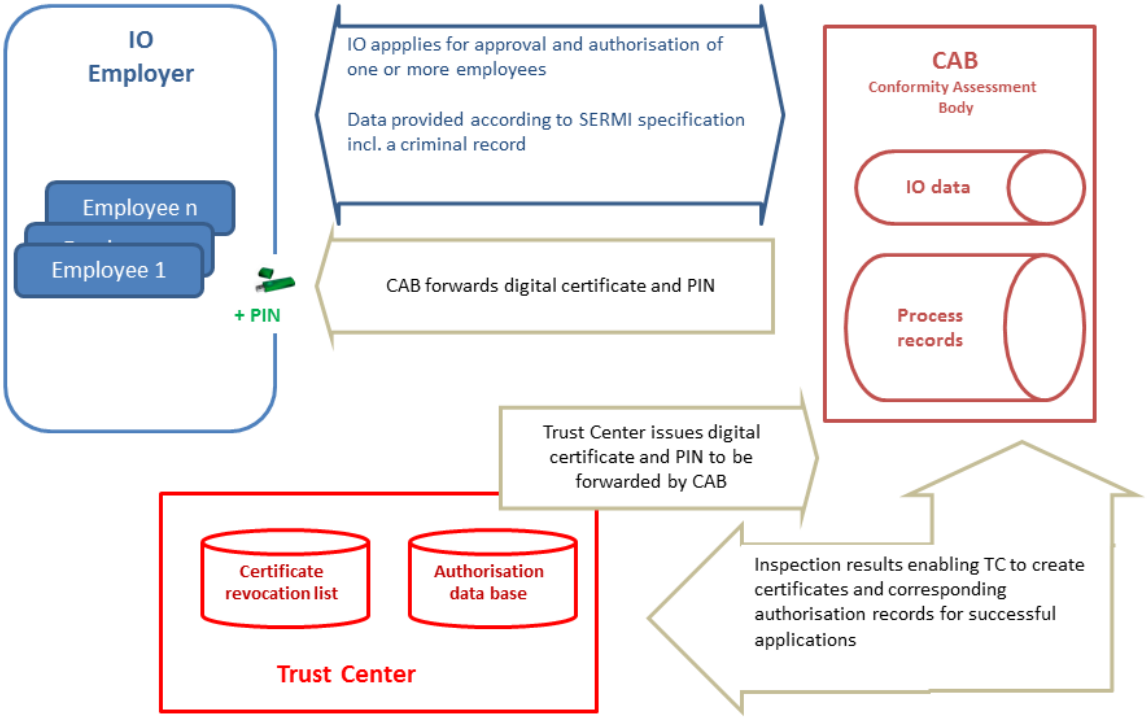

Figure 2: IO approval and IO employee authorisation process

3.1. Overview of the access to security-related RMI

Vehicle manufacturers shall provide access to security-related RMI through their RMI website, provided that the IO employees are authorised and are able to produce the authorisation inspection certificate, and that the IO on whose behalf the IO employees are working has an approval inspection certificate.

Manufacturers may offer access to an on-line ordering facility for security-related parts using a specialised application linked to the RMI website to authorised IO employees that work for approved IOs.

Upon receipt of a request for access to an RMI website, the vehicle manufacturers' websites shall require identification through the IO employee unique identifier and request authentication. Authentication of IO employees shall be carried out exclusively using digital certificates. Upon receipt of a digital certificate, vehicle manufacturer RMI websites shall verify the IO employee unique identifier and the current status of the digital certificate and authorisation, by communicating with the trust centre identified in the digital certificate.

All digital data transfers between IOs, vehicle manufacturers, TCs and CABs shall be carried out via business to business (B2B) transactions, using secure protocols and in a timely manner. Once the IO employee unique identifier and authorisation status of the IO employee have been verified, access to the required security-related RMI shall be provided by the vehicle manufacturer through its website.

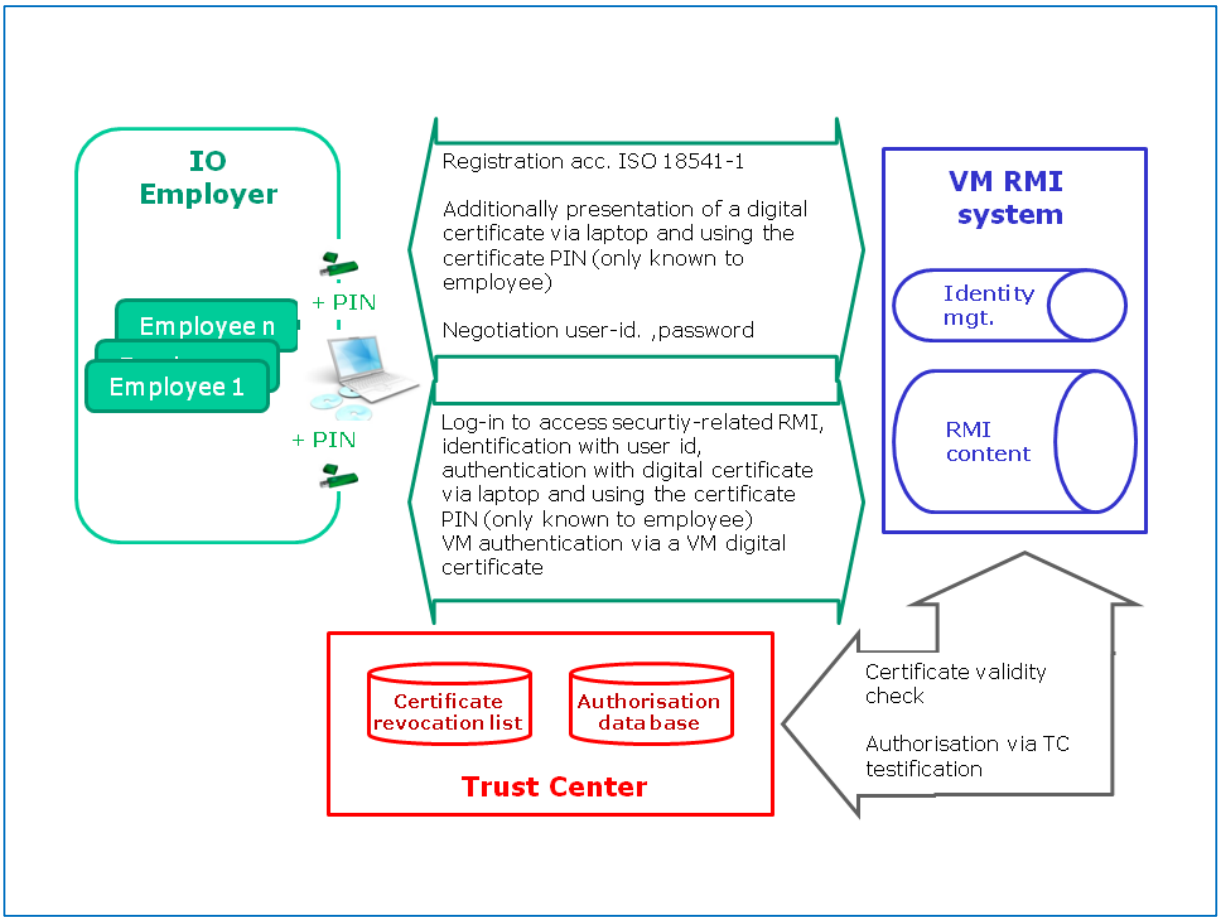

Figure 3: Access to security-related RMI

4. Detailed rules concerning access to security-related RMI

4.1. The role of SERMI

4.1.1. Responsibilities and obligations

(1) SERMI shall advise the Commission on requests for changes to the accreditation process. SERMI shall monitor the implementation of the accreditation process across the Member States and inform the Commission accordingly.

(2) SERMI shall consult the Commission on the creation of the TC selection criteria.

(3) SERMI shall, advise the Commission on the introduction of technical implementation guidelines for interaction between the entities involved in the process.

(4) SERMI shall follow the EA's rules on scheme ownership.

(5) 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.

4.1.2. Trust centre selection

The TC shall be selected by SERMI and be notified to the Commission for approval.

Selected TC shall comply with standard ETSI TS 319 411-3, fulfill the requirements on electronic signatures laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council[7] and the requirements laid down in point 6.6 of this Appendix.

In addition, the TC shall:

– have the technical and managerial competence, and the financial viability and experience relevant to the accreditation process

– have key personnel that has the skills, experience and availability necessary for the accreditation process;

– be able to operate across Member States;

– have in place a quality assurance process at operational level.

4.2. The role of NABs

The NAB shall be responsible for the accreditation of CABs for the purposes of approving IOs and authorising IO employees for access to security-related RMI.

4.2.1. Responsibilities and requirements

The responsibilities and requirements of the NAB are set out in Articles 8 to 12 of Regulation (EC) No 765/2008.

4.2.2. Criteria for CAB accreditation

CABs shall be accredited as type A inspection bodies in accordance with ISO/IEC 17020:2012. CABs shall comply with the requirements concerning the highest level of independence.

Additionally, the NAB shall assess CABs' capability to comply with the requirements laid down in point 4.3.1 and the functional requirements described in point 4.3.2 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.

4.3. The role of CABs

The CAB shall be responsible for the inspection of IOs and their respective IO employees and for issuing approval and authorisation inspection certificates in accordance with this Appendix, and for revoking such certificates.

4.3.1. Responsibilities and requirements

(a) CABs shall keep the data submitted for the approval of an IO;

(b) CABs shall establish a secure communication channel with the TC and provide the inspection results to the TC in order to issue the secure hardware token with a digital certificate;

(c) CABs shall notify IO employees 6 months before their authorisation expires;

[7] 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 repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

(d) CABs shall maintain a database containing data submitted for the authorisation of IO employees;

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

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

(g) CABs shall keep all data relating to IO and IO employees confidential and shall ensure that only unauthorised employees have access to such data;

(h) 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;

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

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

(k) IOs and IO 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;

(l) CABs shall notify IOs 6 months before their approval expires.

(m) CABs shall make random und unannounced on-site inspections of IOs within the 60 months approval validity period, and subject each approved IO to at least one random, on-site inspection over the 60 months approval validity period.

(n) On the basis of a complaint against an approved IO or an authorised IO employee, CABs shall check that the concerned IO or IO 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 on-site inspection is required.

(o) For the purposes of on-site inspections, CABs may request the assistance of market surveillance authorities from the Member State they are established.

(p) CABs shall revoke IO approvals and IO employee authorisations where they no longer comply with the criteria against which they were respectively approved or authorised. CABs shall accordingly request the TC to suspend and repeal digital certificate of the concerned IO employees.

4.3.2. Renewal of the approval

CABs shall, upon request by an IO 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.

CABs shall issue a new approval inspection certificate for IO that fulfils the approval criteria.

CABs shall assess applications for renewals of authorisations and issue an authorisation inspection certificate to IO employees fulfilling the authorisation criteria.

4.3.3. Criteria for IO approval by the CAB

Before approving an IO and during any on-site inspection during the approval validity period, CABs shall check the following:

(6) (a) documented ownership of IO, name of managing director.

(7) (b) the list provided by the IO of employees to be authorised;

(8) (c) information about the responsibility and the function of employees referred to in point (a);

(9) (d) whether the IO 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;

(10) (e) whether the approval of the IO has been revoked for reasons of misuse.

(11) (f) whether the IO has provided proof of activity in the automotive area;

(12) (g) whether the declaration certifying that the IO pursues a legitimate business activity as referred to in point 6.3 has been signed by the IO and during an on-sire inspection whether the IO effectively conducts a legitimate business activity;

(13) (h) whether the IO or the IO employees have a clean criminal record;

(14) (i) whether there is declaration signed by the IO legal representative that compliance with the procedural requirements laid down in point 4.3.4 is ensured for all operations related to vehicle security;

4.3.4. Criteria for IO employee authorisation by the CAB

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

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

(b) that the employee has a clean criminal record;

(c) that there is an employment agreement between the employee concerned and an approved IO;

(d) that the employee concerned has a valid country specific identity card or an equivalent document.

4.4. Role of the IOs

4.4.1. Responsibilities and requirements

(15) (a) IOs shall request an inspection from their CAB to obtain approval;

(16) (b)IOs shall inform their CAB about changes in their contact details;

(17) (c) IOs shall inform their CAB when their business is dissolved;

(18) (d)IOs shall record every security related RMI transaction and operation;

(19) (e) IOs shall inform their CAB of any termination of employment of any of their authorised employees;

(20) (f) IOs shall report to the relevant authorities any offence or misconduct that has been committed by their authorised employees and that is concerns security related RMI;

(21) (g)IOs shall ensure that their authorised employees only use their own authorisation inspection certificates;

(22) (h)IOs shall ensure that all fees relating to their IO employee's authorisation have been paid;

(23) (i) IOs shall ensure that their IO employees are trained for repair activities concerning automotive maintenance, reprogramming and security and safety functions;

(24) (j) IO shall request their CAB for an on-site inspection in the six months prior to the expiration of their approval inspection certificate.

4.5. Role of IO employees

.

4.5.1. Responsibilities and requirements

(25) (a) IO employees shall request their CAB for authorisation

(26) (b)IO employees shall register themselves on the vehicle manufacturer's RMI system;

(27) (c) IO employees shall access secure related RMI in accordance with ISO standard 18541 – 2014;

(28) (d)IO 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;

(29) (e) where applicable, IO employees shall notify their IO employer that their digital certificate is no longer required;

(30) (f)IO employee shall not share with any third party the secure software token, the digital certificate or the PIN;;

(31) (g)IO employees shall be responsible for using the personal secure software token and PIN correctly;

(32) (h)IO employees shall inform their IO and their TC about any loss or misuse of their secure hardware token within 24 hours of such loss or misuse;

(33) (i) IO employees shall report to the relevant authorities any request or act from other IO employees relating to secure RMI that does not constitute a legitimate business activity as referred to in point 6.3. of this Annex.

4.6. Role of the trust centre

TCs shall create and send the digital certificates to the IOs via the respective CABs to the IOs and the IO employees. TCs shall maintain a database of issued inspection authorisation certificates. TCs shall provide vehicle manufactures access to an interface to verify the status of the digital certificates and the inspection authorisation certificates.

TCs shall keep the information regarding IO 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 where the IO employee is working.

4.6.1. Responsibilities and requirements

(a) TCs can suspend and repeal digital certificates upon request from the CAB;

(b) TCs shall provide the software to use the digital certificates to the IO and IO employees;

(c) TCs shall operate 24 hours a day, 7 days a week;

4.7. Role of vehicle manufacturers

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

4.7.1. Responsibilities and requirements

(34) (a) vehicle manufacturers shall ensure that their websites are adapted to support the access of IOs to security-related RMI;

(35) (b) vehicle manufacturers shall ensure that they download the latest software updates made available on the SERMI website.

(36)

4.7.2. Procedural requirements for vehicle manufacturers

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

(37) (a) procedural requirements for stolen vehicles.

Vehicle manufacturers shall keep a record of all vehicles of its brand reported as stolen by the authorities.

Vehicle manufactures 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.

(b) Procedural requirements for storing information

Vehicle manufacturers shall store the following information for each access granted to security-related repair and maintenance information:

(38) (a) the Vehicle Identification Number (VIN) of the vehicle for which the information was requested;

(39) (b) the date the request was made;

(40) (c) the vehicle registration number of the vehicle for which the information was requested, where available;

(41) (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.