Consiglio
dell'Unione europea

Bruxelles, 20 maggio 2021
(OR. en)

8978/21
ADD 1

ENT 85
MI 370
DELACT 105

NOTA DI TRASMISSIONE

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	20 maggio 2021
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, segretario generale del Consiglio dell'Unione europea
n. doc. Comm.:	C(2021) 3377 final, ANNEX
Oggetto:	ALLEGATO del regolamento delegato (UE) .../... della Commissione che modifica l'allegato X del regolamento (UE) 2018/858 del Parlamento europeo e del Consiglio per quanto riguarda l'accesso standardizzato alle informazioni diagnostiche di bordo dei veicoli e alle informazioni sulla riparazione e la manutenzione dei veicoli, nonché le prescrizioni e le procedure riguardo all'accesso alle informazioni relative alla sicurezza dei veicoli

Si trasmette in allegato, per le delegazioni, il documento C(2021) 3377 final, ANNEX.

All.: C(2021) 3377 final, ANNEX

COMMISSIONE
EUROPEA

Bruxelles, 20.5.2021
C(2021) 3377 final

ANNEX

ALLEGATO

del

regolamento delegato (UE) .../... della Commissione

che modifica l'allegato X del regolamento (UE) 2018/858 del Parlamento europeo e del Consiglio per quanto riguarda l'accesso standardizzato alle informazioni diagnostiche di bordo dei veicoli e alle informazioni sulla riparazione e la manutenzione dei veicoli, nonché le prescrizioni e le procedure riguardo all'accesso alle informazioni relative alla sicurezza dei veicoli

ALLEGATO

L'allegato X del regolamento (UE) 2018/858 è così modificato:

(1) il punto 2.1 è sostituito dal seguente:

"2.1. A norma dell'articolo 61, paragrafo 2, secondo comma, prima frase, un costruttore attua le disposizioni e le procedure necessarie a garantire che le informazioni OBD del veicolo e le informazioni sulla riparazione e la manutenzione del veicolo siano accessibili su siti web. Si ritiene che i costruttori adempiano l'obbligo di fornire sui loro siti web in un formato standardizzato informazioni OBD e informazioni sulla riparazione e la manutenzione del veicolo conformandosi alla parte 1 "Informazioni generali e definizione dei casi di utilizzo", alla parte 2 "Requisiti tecnici" e alla parte 3 "Requisiti funzionali dell'interfaccia per l'utilizzatore" della norma EN ISO 18541-2014, alla parte 4 "Prove di conformità" della norma EN ISO 18541-2015 e alla parte 5 "Disposizioni specifiche per veicoli pesanti — Veicoli stradali - Accesso normalizzato alle informazioni sulla riparazione e manutenzione degli autoveicoli (RMI)" della norma EN ISO 18541-2018. L'accesso alle informazioni OBD del veicolo e alle informazioni sulla riparazione e la manutenzione del veicolo deve essere consentito in modo rapido e semplice.";

(2) il punto 2.5.2 è sostituito dal seguente:

"2.5.2. manuali di servizio, compresi i registri per annotare riparazioni e attività di manutenzione, e riferimenti delle specifiche tecniche riguardanti i liquidi, compresi lubrificanti, liquidi per freni e liquidi di raffreddamento;";

(3) al punto 2.9, il primo comma è sostituito dal seguente:

"Ai fini dell'OBD, della diagnostica, della riparazione e manutenzione, del monitoraggio e dell'ispezione dei veicoli, il flusso di dati diretto del veicolo, comprendente i codici di guasto, e le funzioni diagnostiche devono essere resi disponibili attraverso la porta seriale del connettore normalizzato per la trasmissione dati indicato al punto 6.5.1.4, conformemente alle specifiche di cui all'allegato 11, appendice 1, punto 6.5.3 del regolamento n. 83 della Commissione economica per l'Europa delle Nazioni Unite (UNECE)[1], all'allegato 9B, punto 4.7.3, del regolamento n. 49 della Commissione economica per l'Europa delle Nazioni Unite (UN/ECE)[2] e alle norme di riferimento di cui all'appendice 6 del medesimo allegato 9B.";

(4) al punto 6.1, il primo comma è sostituito dal seguente:

"Si presume che i costruttori adempiano l'obbligo di fornire le informazioni OBD del veicolo e le informazioni sulla riparazione e la manutenzione del

[1] Regolamento n. 83 della Commissione economica per l'Europa delle Nazioni Unite (UNECE) — Disposizioni uniformi relative all'omologazione dei veicoli per quanto riguarda le emissioni inquinanti in base al carburante utilizzato dal motore (GU L 42 del 15.2.2012, pag. 1).

[2] Regolamento n. 49 della Commissione economica per l'Europa delle Nazioni Unite (UN/ECE) — Prescrizioni uniformi relative ai provvedimenti da prendere contro le emissioni di inquinanti gassosi e di particolato prodotte dai motori ad accensione spontanea e dai motori ad accensione comandata destinati alla propulsione di veicoli (GU L 180 dell'8.7.2011, pag. 53).

veicolo sui loro siti web in un formato standardizzato conformandosi alle parti della norma EN ISO 18541 di cui al punto 2.1.";

(5) il punto 6.2 è sostituito dal seguente:

"L'accesso alle funzioni di sicurezza del veicolo deve essere reso disponibile agli operatori indipendenti con la protezione di una tecnologia di sicurezza nel rispetto delle seguenti prescrizioni:";

(6) il punto 6.3 è così modificato:

(a) la prima frase è sostituita dalla seguente:

"La procedura di cui al punto 6.2 per approvare gli operatori indipendenti e autorizzarne l'accesso alle funzioni di sicurezza del veicolo è stabilita al punto 6.2 dell'appendice 3. Il ruolo e le responsabilità degli organismi che partecipano all'accreditamento, all'approvazione e all'autorizzazione degli operatori indipendenti sono specificati mediante prescrizioni funzionali sotto forma di esempi e casi d'uso di cui nella comunicazione della Commissione ....";

(b) è aggiunto il seguente comma:

"Ai fini di tale procedura, si ritiene che gli operatori non esercitino un'attività commerciale legittima se pubblicizzano o offrono operazioni di riparazione o manutenzione che inciderebbero negativamente sulle prestazioni del veicolo dal punto di vista delle emissioni. Tali operazioni includono:

(a) disattivare o rimuovere dispositivi antinquinamento o sistemi di controllo delle emissioni, o degradarne le prestazioni o occultarne il cattivo funzionamento;

(b) installare impianti di manipolazione[3] o strategie di manomissione[4];

(c) disattivare, rimuovere o manomettere dispositivi per il monitoraggio del consumo di carburante o di energia elettrica, o manomettere le indicazioni del contachilometri;

(d) manomettere la centralina del motore, anche per quanto riguarda la potenza nominale del motore.";

(7) è aggiunta la seguente appendice 3:

"Appendice 3

Procedura di approvazione e autorizzazione degli operatori indipendenti ai fini dell'accesso alle funzioni di sicurezza del veicolo[5]

1. Ambito di applicazione

La presente appendice reca le prescrizioni ai fini dell'approvazione e dell'autorizzazione degli operatori indipendenti che richiedono l'accesso alle informazioni sulla riparazione e la manutenzione dei veicoli (RMI) connesse alla sicurezza.

---

3 Come definiti all'articolo 3, punto 10, del regolamento (CE) n. 715/2007.

4 Come definite all'articolo 3, punto 8, del regolamento (CE) n. 595/2009.

5 Le prescrizioni stabilite nella presente appendice sono basate su quanto stabilito nel programma di accreditamento, approvazione e autorizzazione ai fini dell'accesso alle informazioni sulla riparazione e la manutenzione (RMI) relative alla sicurezza convalidato il 19 maggio 2016 dalla Cooperazione europea per l'accreditamento (https://www.vehiclesermi.eu/).

In essa sono indicati in dettaglio il processo e gli organismi necessari per l'approvazione e l'autorizzazione degli operatori indipendenti ai fini della concessione dell'accesso alle informazioni sulla riparazione e la manutenzione (RMI) del veicolo connesse alla sicurezza per quanto riguarda i veicoli passeggeri e commerciali leggeri e i veicoli pesanti.

2. Definizioni e abbreviazioni

2.1. Definizioni

Ai fini della presente appendice si applicano le seguenti definizioni:

2.1.1. "Accreditamento"

Per "accreditamento" si intende l'accreditamento come definito all'articolo 2, punto 10, del regolamento (CE) n. 765/2008.

2.1.2. "Dipendente di un OI"

Per "dipendente di un OI" si intende il dipendente di un operatore indipendente (OI) approvato che, previa autorizzazione dell'organismo di valutazione della conformità competente (CAB - *Conformity Assessment Body*), avrà accesso alle RMI connesse alla sicurezza.

2.1.3. "Informazioni sulla riparazione e la manutenzione connesse alla sicurezza" o "RMI connesse alla sicurezza"

Per "informazioni sulla riparazione e la manutenzione connesse alla sicurezza" o "RMI connesse alla sicurezza" si intendono le informazioni, il software, le funzioni e i servizi necessari per la riparazione e la manutenzione delle funzioni inserite in un veicolo dal costruttore per prevenire il furto o la sottrazione del veicolo e consentire di rintracciarlo e recuperarlo.

2.1.4. "Certificato ispettivo di approvazione"

Per "certificato ispettivo di approvazione" si intende il certificato rilasciato dal CAB agli OI che soddisfano i criteri per l'approvazione stabiliti nella presente appendice che conferma che tali OI sono approvati e che i relativi dipendenti possono richiedere l'autorizzazione ad accedere alle RMI connesse alla sicurezza.

2.1.5. "Certificato ispettivo di autorizzazione"

Per "certificato ispettivo di autorizzazione" si intende il certificato rilasciato dal CAB ai dipendenti di un OI che soddisfano i criteri per l'autorizzazione stabiliti nella presente appendice che conferma che tali dipendenti sono autorizzati ad accedere alle RMI connesse alla sicurezza sul sito web di un costruttore di veicoli.

2.1.6. "Centro protezione" o "TC" (*Trust Centre*)

Per "centro protezione" o "TC" si intende l'organismo designato dal SERMI e approvato dalla Commissione che è responsabile di quanto elencato di seguito:

a) gestione dei certificati digitali e dello status dell'autorizzazione dei dipendenti di un OI e fornitura al CAB dei token di sicurezza e dei certificati digitali necessari per i dipendenti autorizzati di un OI;

b) fornitura al costruttore dei veicoli delle informazioni relative allo status dell'autorizzazione di un dipendente di un OI.

2.1.7. "Token di sicurezza"

Per "token di sicurezza" si intende un dispositivo che consente l'autenticazione sicura di un OI.

2.1.8. "Certificato digitale"

Per "certificato digitale" si intende un certificato digitale che richiede una firma digitale del centro protezione che lo rilascia per vincolare una chiave pubblica all'identità del dipendente di un OI conformemente alla norma ISO 9594.

2.1.9. "Banca dati delle autorizzazioni"

Per "banca dati delle autorizzazioni" si intende una banca dati detenuta dal centro protezione che contiene le informazioni anonimizzate sulle autorizzazioni dei dipendenti autorizzati di un OI e la registrazione degli OI approvati.

2.1.10. "Banca dati delle certificazioni"

Per "banca dati delle certificazioni" si intende una banca dati detenuta dal centro protezione per gestire la validità dei certificati digitali e gli identificatori dei dipendenti autorizzati di un OI.

2.1.11. "Cooperazione europea per l'accreditamento" o "EA"

Per "Cooperazione europea per l'accreditamento" o "EA" si intende l'organismo riconosciuto dalla Commissione conformemente all'articolo 14 del regolamento (CE) n. 765/2008 responsabile dello sviluppo, del mantenimento e dell'attuazione dell'accreditamento nell'Unione.

2.1.12. "Forum per l'accesso alle RMI del veicolo connesse alla sicurezza" o "SERMI"

Per "Forum per l'accesso alle RMI del veicolo connesse alla sicurezza" o "SERMI" si intende l'entità incaricata delle attività di coordinamento e consulenza per la Commissione in merito all'attuazione delle procedure di accreditamento, approvazione e autorizzazione ai fini dell'accesso alle RMI connesse alla sicurezza.

2.1.13. "Autorità competenti"

Per "autorità competenti" si intendono le autorità pubbliche provviste di un mandato giuridico per agire nel settore della protezione, dell'indagine e del perseguimento dei reati in materia di sicurezza dei veicoli.

3. Accreditamento dei CAB, approvazione degli OI e autorizzazione dei dipendenti di un OI

Solo i CAB accreditati dall'organismo nazionale di accreditamento ("NAB" - *National Accreditation Body*), quale definito all'articolo 2, punto 11, del regolamento (CE) n. 765/2008, dello Stato membro in cui sono stabiliti rilasciano certificati ispettivi di approvazione attestanti che un OI è stato approvato e certificati ispettivi di autorizzazione attestanti che un dipendente di un OI può avere accesso alle RMI connesse alla sicurezza.

L'approvazione dell'OI e l'autorizzazione del suo dipendente sono concesse per un periodo di 60 mesi a decorrere dalla data di rilascio dei relativi certificati ispettivi.

Gli OI che desiderano ricevere RMI connesse alla sicurezza devono ottenere un certificato ispettivo di approvazione da un CAB accreditato dal NAB dello Stato membro in cui sono stabiliti.

I dipendenti di un OI che tratteranno le RMI connesse alla sicurezza devono ottenere un certificato ispettivo di autorizzazione da un CAB accreditato dal NAB dello Stato membro in cui risiedono.

I CAB informano i TC del rilascio di ogni certificato ispettivo di approvazione o certificato ispettivo di autorizzazione. Ricevuta la comunicazione, i TC registrano l'autorizzazione e rilasciano un token di sicurezza e un certificato digitale contenenti le informazioni che consentono ai dipendenti di un OI di essere identificabili in modo univoco sul sito web RMI del costruttore del veicolo. I CAB devono fornire ai singoli dipendenti di un OI un token di sicurezza e il certificato digitale.

I costruttori dei veicoli possono chiedere un canone per la registrazione dei dipendenti di un OI sui loro siti web RMI e per l'accesso alle RMI connesse alla sicurezza. Tale canone deve essere proporzionato al costo della registrazione e della fornitura dell'accesso. I canoni dovuti devono essere indicati sui siti web RMI dei costruttori dei veicoli. Tutti i trasferimenti digitali di dati tra OI, TC e CAB devono essere effettuati tramite transazioni tra imprese (B2B), in maniera tempestiva e utilizzando protocolli sicuri.

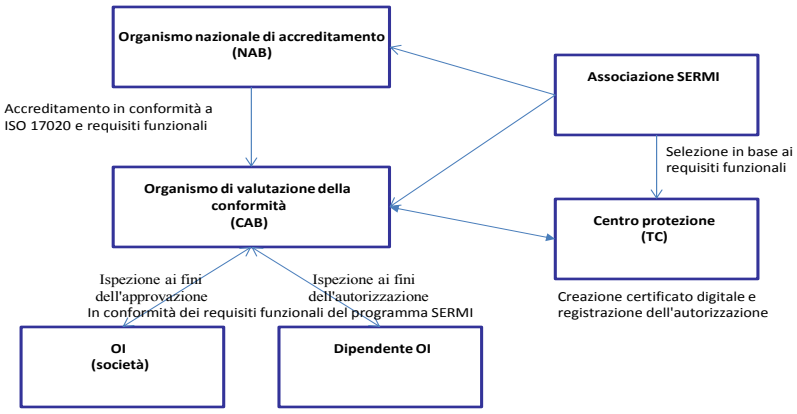

Figura 1: organismi che partecipano all'accreditamento dei CAB, all'approvazione degli OI e all'autorizzazione dei dipendenti di un OI, e rapporti tra di loro

L'OI che richiede l'autorizzazione al CAB deve firmare una dichiarazione attestante che esercita un'attività commerciale legittima, di cui al punto 6.3 del presente allegato. Un OI è approvato solo previa ispezione da parte del CAB che verifica che tale dichiarazione sia firmata e che valuta la conformità dell'OI e dei suoi singoli dipendenti alle prescrizioni stabilite nella presente appendice.

I singoli dipendenti di un OI sono autorizzati esclusivamente previa ispezione da parte di un CAB. Il CAB controlla i documenti presentati e verifica se il dipendente di un OI in questione ha già presentato in precedenza una richiesta di autorizzazione respinta dal CAB interessato o da qualsiasi altro CAB a livello di Unione.

I CAB trasmettono tutti i dati di cui necessita il TC per produrre il certificato digitale e il token di sicurezza, che il CAB trasmette ai dipendenti di un OI.

I dipendenti di un OI che sono stati autorizzati ricevono dal CAB competente il PIN associato al certificato digitale.

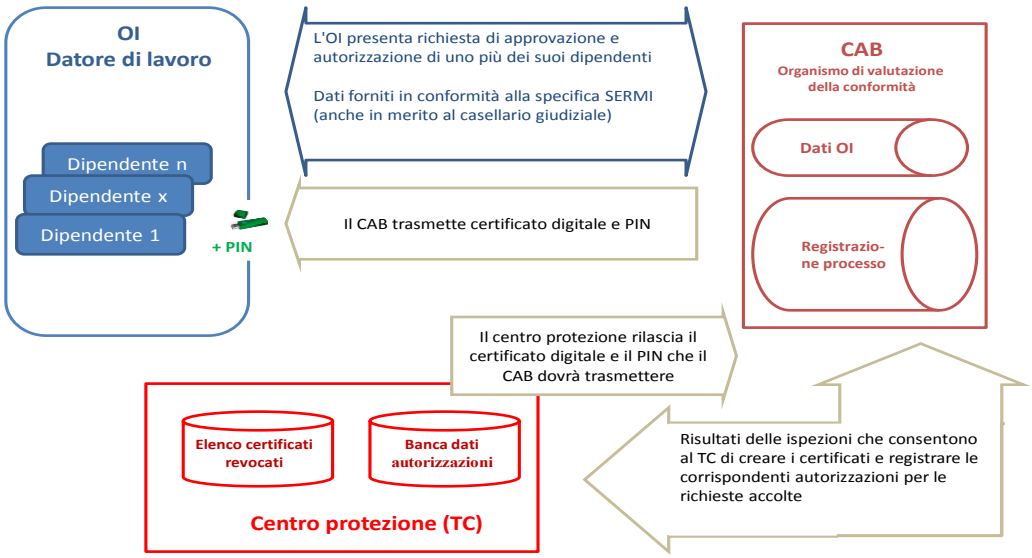

Figura 2: processo di approvazione dell'OI e di autorizzazione del dipendente di un OI

3.1. Panoramica dell'accesso alle RMI connesse alla sicurezza

I costruttori dei veicoli consentono l'accesso alle RMI connesse alla sicurezza attraverso il loro sito web RMI, a condizione che i dipendenti dell'OI siano autorizzati e siano in grado di presentare il certificato ispettivo di autorizzazione, e che l'OI per conto del quale operano sia in possesso di un certificato ispettivo di approvazione.

I costruttori possono offrire ai dipendenti autorizzati di un OI che lavorano per OI approvati l'accesso a un dispositivo on-line per ordinare componenti legati alla sicurezza utilizzando un'applicazione specifica collegata al sito web RMI.

Quando ricevono una richiesta di accesso a un sito web RMI, i siti web dei costruttori dei veicoli devono richiedere sia l'identificazione tramite identificatore unico del dipendente di un OI sia l'autenticazione. L'autenticazione dei dipendenti di un OI deve essere effettuata esclusivamente per mezzo di certificati digitali. Quando ricevono un certificato digitale, i siti web dei costruttori dei veicoli devono verificare l'identificatore unico del dipendente dell'OI e lo status aggiornato del certificato digitale e dell'autorizzazione, comunicando con il TC indicato nel certificato digitale.

Tutti i trasferimenti digitali di dati tra OI, costruttori dei veicoli, TC e CAB devono essere effettuati tramite transazioni tra imprese (B2B), in maniera tempestiva e utilizzando protocolli sicuri. Una volta verificati l'identificatore unico e lo status dell'autorizzazione del dipendente dell'OI, il costruttore dei veicoli deve consentire l'accesso alle RMI connesse alla sicurezza attraverso il proprio sito web.

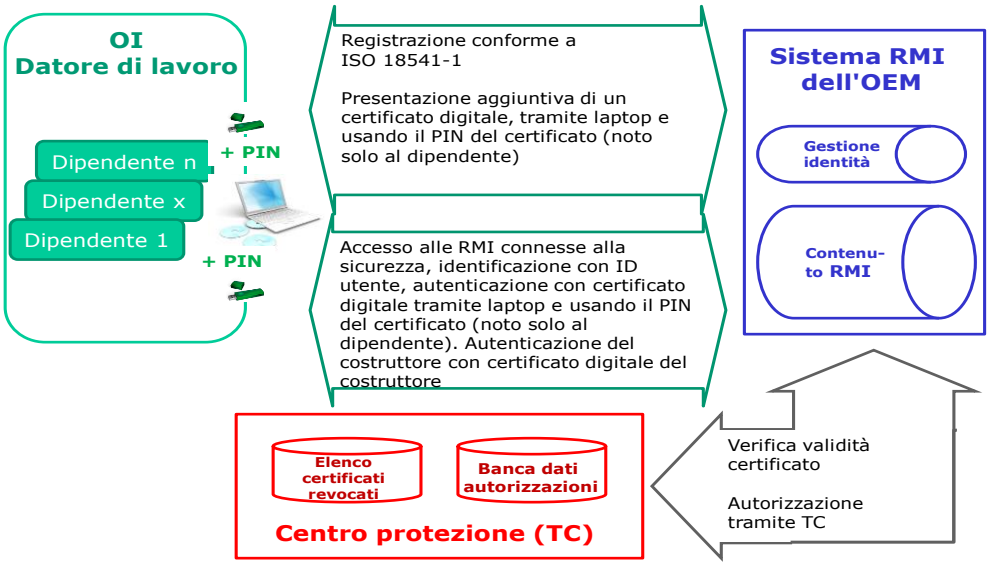

Figura 3: accesso alle RMI connesse alla sicurezza

4. Norme dettagliate relative all'accesso alle RMI connesse alla sicurezza

4.1. Ruolo del SERMI

4.1.1. Responsabilità e obblighi

Il SERMI monitora l'attuazione del processo di accreditamento in tutti gli Stati membri e ne informa la Commissione. Il SERMI fornisce consulenza alla Commissione in merito alle richieste di modifica del processo di accreditamento.

(a) Il SERMI fornisce consulenza alla Commissione in merito alle richieste di modifica del processo di accreditamento. Il SERMI monitora l'attuazione del processo di accreditamento in tutti gli Stati membri e ne informa la Commissione.

(b) Il SERMI consulta la Commissione in merito all'elaborazione dei criteri di selezione dei TC.

(c) Il SERMI fornisce consulenza alla Commissione sull'introduzione di orientamenti tecnici di attuazione per l'interazione tra le entità che partecipano al processo.

(d) Il SERMI si attiene alle norme della EA per quanto concerne la proprietà del programma.

(e) I membri del SERMI sono rappresentati dai portatori di interessi impegnati nel processo di accreditamento, approvazione e autorizzazione ai fini dell'accesso alle RMI connesse alla sicurezza.

4.1.2. Selezione del centro protezione (TC)

Il centro protezione è selezionato dal SERMI e comunicato alla Commissione per l'approvazione.

I centri protezione selezionati devono rispettare la norma ETSI TS 319 411-3, le prescrizioni in materia di firme elettroniche sancite dal regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio[6] e le prescrizioni stabilite al punto 4.6 della presente appendice.

Il centro protezione deve inoltre:

– disporre della competenza tecnica e gestionale, oltre che dell'adeguata capacità finanziaria ed esperienza ai fini del processo di accreditamento;

– disporre di personale chiave dotato delle competenze, dell'esperienza e della disponibilità necessarie ai fini del processo di accreditamento;

– essere in grado di operare in tutti gli Stati membri;

– disporre di un processo di garanzia della qualità a livello operativo.

4.2. Ruolo dei NAB

I NAB sono responsabili dell'accreditamento dei CAB ai fini dell'approvazione degli OI e dell'autorizzazione dei dipendenti degli OI per l'accesso alle RMI connesse alla sicurezza.

4.2.1. Responsabilità e prescrizioni

Le responsabilità dei NAB e le prescrizioni cui sono sottoposti sono stabilite negli articoli da 8 a 12 del regolamento (CE) n. 765/2008.

4.2.2. Criteri per l'accreditamento dei CAB

I CAB devono essere accreditati in qualità di organismi di ispezione di tipo A conformemente alla norma ISO/IEC 17020:2012. I CAB devono osservare le prescrizioni relative al massimo livello di indipendenza.

I NAB devono inoltre valutare la capacità dei CAB di osservare le prescrizioni stabilite ai punti da 4.3.1 a 4.3.4.

Il personale incaricato delle ispezioni degli OI deve disporre di un livello di conoscenze adeguato ai compiti da svolgere per quanto concerne il settore della riparazione e della manutenzione dei veicoli e le specifiche post-vendita del settore automobilistico.

4.3. Ruolo dei CAB

I CAB sono responsabili dell'ispezione degli OI e dei relativi dipendenti e del rilascio dei certificati ispettivi di approvazione e di autorizzazione in conformità alla presente appendice, nonché della revoca di tali certificati.

4.3.1. Responsabilità e prescrizioni

(a) I CAB devono conservare i dati presentati per l'approvazione degli OI.

[6] Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (GU L 257 del 28.8.2014, pag. 73).

(b) I CAB devono stabilire un canale di comunicazione sicuro con il TC e trasmettere al TC i risultati delle ispezioni ai fini del rilascio del token di sicurezza con un certificato digitale.

(c) I CAB devono inviare una notifica ai dipendenti degli OI 6 mesi prima della scadenza della loro autorizzazione.

(d) I CAB devono mantenere una banca dati contenente i dati presentati per l'autorizzazione dei dipendenti degli OI.

(e) I CAB che rifiutano di approvare un OI o di autorizzare un dipendente di un OI devono comunicare al TC i risultati dell'ispezione relativi a tale OI o dipendente di un OI.

(f) I CAB devono raccogliere e utilizzare solo i dati necessari per il processo di approvazione o di autorizzazione.

(g) I CAB devono garantire la riservatezza di tutti i dati relativi agli OI e ai dipendenti degli OI e fare sì che solo il personale autorizzato abbia accesso a tali dati.

(h) I CAB devono fornire una volta l'anno al SERMI e alla Commissione le statistiche relative al numero di approvazioni e autorizzazioni rilasciate, nonché al numero di rifiuti.

(i) I CAB devono conservare per un periodo di 5 anni registri sicuri delle ispezioni a fini di approvazione e autorizzazione.

(j) I CAB devono informare tutti gli altri CAB dello Stato membro in cui è stabilito un OI oggetto di un'ispezione se tale ispezione ha dato risultati negativi.

(k) Gli OI e i dipendenti di un OI oggetto di un'ispezione che ha dato risultati negativi possono fornire al CAB informazioni supplementari volte a rettificare carenze di lieve entità entro 15 giorni lavorativi dal ricevimento del risultato negativo dell'ispezione. I CAB devono stabilire di conseguenza se occorre modificare il risultato dell'ispezione.

(l) I CAB devono inviare una notifica agli OI 6 mesi prima della scadenza della loro approvazione.

(m) I CAB devono eseguire ispezioni casuali in loco senza preavviso presso gli OI entro i 60 mesi del periodo di validità dell'approvazione e sottoporre ciascun OI approvato quanto meno a un'ispezione casuale in loco nel corso dei 60 mesi del periodo di validità dell'approvazione.

(n) Sulla base di una denuncia nei confronti di un OI approvato o di un dipendente di un OI autorizzato, i CAB devono verificare che l'OI o il dipendente di un OI in questione soddisfino i criteri in base ai quali era stata loro concessa, rispettivamente, l'approvazione o l'autorizzazione. Il CAB decide nel corso delle proprie indagini se è necessaria o no un'ispezione in loco.

(o) Ai fini delle ispezioni in loco i CAB possono chiedere l'assistenza delle autorità di vigilanza del mercato dello Stato membro in cui sono stabiliti.

(p) I CAB devono revocare le approvazioni degli OI e le autorizzazioni dei dipendenti di un OI se detti OI o dipendenti di un OI non soddisfano più i criteri in base ai quali era stata loro concessa, rispettivamente, l'approvazione o

l'autorizzazione. I CAB devono chiedere di conseguenza al TC di sospendere e abrogare il certificato digitale dei dipendenti di un OI interessati.

4.3.2. Rinnovo dell'approvazione

Su richiesta di un OI o 6 mesi prima della scadenza della validità dell'approvazione, i CAB eseguono un'ispezione in loco e, in caso di risultato positivo, rinnovano l'approvazione.

I CAB rilasciano un nuovo certificato ispettivo di approvazione all'OI che soddisfa i criteri per l'approvazione.

I CAB valutano le richieste di rinnovo delle autorizzazioni e rilasciano un certificato ispettivo di autorizzazione ai dipendenti di un OI che soddisfano i criteri per l'autorizzazione.

4.3.3. Criteri per l'approvazione degli OI da parte dei CAB

Prima di concedere l'approvazione a un OI e nel corso di qualsiasi ispezione in loco durante il periodo di validità dell'approvazione, i CAB devono controllare quanto segue:

(a) proprietà documentata dell'OI, nome dell'amministratore;

(b) elenco fornito dall'OI dei dipendenti da autorizzare;

(c) informazioni sulla responsabilità e sulla funzione dei dipendenti di cui alla lettera a);

(d) se l'OI dispone di un'assicurazione di responsabilità civile con un importo minimo di copertura di 1 milione di EUR per lesioni personali e di 0,5 milioni di EUR per danni materiali;

(e) se l'approvazione dell'OI è stata revocata per uso improprio;

(f) se l'OI ha fornito prove della sua attività nel settore automobilistico;

(g) se la dichiarazione attestante che l'OI esercita un'attività commerciale legittima di cui al punto 6.3 è stata firmata dall'OI e, nel corso di un'ispezione in loco, se l'OI esercita effettivamente un'attività commerciale legittima;

(h) se l'OI o i dipendenti di un OI hanno precedenti penali;

(i) se è disponibile una dichiarazione firmata dal rappresentante legale dell'OI attestante che la conformità alle prescrizioni procedurali di cui al punto 4.3.4 è assicurata per tutte le operazioni relative alla sicurezza dei veicoli.

4.3.4. Criteri per l'autorizzazione dei dipendenti degli OI da parte dei CAB

Prima di autorizzare un dipendente come dipendente di un OI e nel corso di qualsiasi ispezione in loco durante il periodo di validità dell'approvazione, i CAB devono verificare quanto segue:

a) che al dipendente in questione non sia stata in precedenza revocata l'autorizzazione per uso improprio;

b) che il dipendente non abbia precedenti penali;

c) che sia in vigore un contratto di lavoro tra il dipendente in questione e un OI approvato;

d) che il dipendente in questione sia in possesso di una carta di identità nazionale valida o di un documento equivalente.

4.4. Ruolo degli OI

4.4.1. Responsabilità e prescrizioni

(a) Gli OI devono chiedere un'ispezione al proprio CAB per ottenere l'approvazione.

(b) Gli OI devono informare il CAB competente in merito alle modifiche dei loro recapiti.

(c) Gli OI devono informare il CAB competente quando cessano la propria attività.

(d) Gli OI devono registrare tutte le operazioni e le transazioni RMI connesse alla sicurezza.

(e) Gli OI devono informare il CAB competente in merito a ogni eventuale risoluzione del contratto dei loro dipendenti autorizzati.

(f) Gli OI devono riferire alle autorità competenti qualsiasi reato o illecito commesso dai loro dipendenti autorizzati relativo alle RMI connesse alla sicurezza.

(g) Gli OI devono garantire che i loro dipendenti autorizzati utilizzino esclusivamente i loro certificati ispettivi di autorizzazione personali.

(h) Gli OI devono garantire che tutti gli oneri relativi all'autorizzazione dei loro dipendenti siano stati pagati.

(i) Gli OI devono garantire che i loro dipendenti siano formati per le attività di riparazione relative alla manutenzione, alla riprogrammazione e alle funzioni di sicurezza degli autoveicoli.

(j) Gli OI devono chiedere al CAB competente un'ispezione in loco nei sei mesi precedenti la scadenza del loro certificato ispettivo di approvazione.

4.5. Ruolo dei dipendenti degli OI

4.5.1. Responsabilità e prescrizioni

(a) I dipendenti degli OI devono chiedere l'autorizzazione al CAB competente.

(b) I dipendenti degli OI devono registrarsi nel sistema RMI del costruttore del veicolo.

(c) I dipendenti degli OI devono accedere alle RMI connesse alla sicurezza nel rispetto della norma EN ISO 18541-2014.

(d) I dipendenti degli OI devono garantire che tutti i registri di RMI connesse alla sicurezza scaricati dal sistema RMI del costruttore del veicolo non siano conservati più di quanto necessario per l'esecuzione dell'operazione per la quale sono necessarie tali informazioni.

(e) Se del caso, i dipendenti degli OI devono comunicare al proprio datore di lavoro che il loro certificato digitale non è più necessario.

(f) I dipendenti degli OI non devono condividere con terzi il token di sicurezza, il certificato digitale o il PIN.

(g) I dipendenti degli OI sono responsabili dell'uso corretto del token di sicurezza e del PIN personali.

(h) I dipendenti degli OI devono informare entro 24 ore i rispettivi OI e TC in caso di smarrimento o di uso improprio dei loro token di sicurezza.

(i) I dipendenti degli OI devono riferire alle autorità competenti qualsiasi richiesta o atto di altri dipendenti di un OI riguardante le RMI connesse alla sicurezza che non costituisca un'attività commerciale legittima ai sensi del punto 6.3 del presente allegato.

4.6. Ruolo del centro protezione (TC)

I TC realizzano e trasmettono i certificati digitali attraverso i rispettivi CAB agli OI e ai loro dipendenti. I TC mantengono una banca dati dei certificati ispettivi di autorizzazione rilasciati. I TC consentono l'accesso dei costruttori dei veicoli a un'interfaccia affinché possano verificare lo status dei certificati digitali e dei certificati ispettivi di autorizzazione.

I TC conservano le informazioni relative ai dipendenti degli OI nella banca dati delle autorizzazioni per un periodo supplementare di 60 mesi al massimo. Tale periodo non può essere superiore al rimanente periodo di validità dell'approvazione concessa all'OI per cui lavora il dipendente.

4.6.1. Responsabilità e prescrizioni

a) I TC possono sospendere e abrogare i certificati digitali su richiesta del CAB.

b) I TC devono fornire agli OI e ai relativi dipendenti il software per utilizzare i certificati digitali.

c) I TC devono essere operativi 24 ore su 24, 7 giorni su 7.

4.7. Ruolo dei costruttori dei veicoli

I costruttori dei veicoli consentono a tutti gli OI approvati e a tutti i dipendenti autorizzati degli OI l'accesso alle informazioni sulla riparazione e la manutenzione connesse alla sicurezza. I costruttori dei veicoli comunicano con i TC per verificare lo status dell'autorizzazione e dell'autenticazione dei dipendenti degli OI che chiedono l'accesso a tali informazioni.

4.7.1. Responsabilità e prescrizioni

(a) I costruttori dei veicoli devono garantire che i loro siti web siano adattati per supportare l'accesso degli OI alle RMI connesse alla sicurezza;

(b) i costruttori dei veicoli devono provvedere a scaricare le specifiche tecniche rese disponibili sul sito web del SERMI.

4.7.2. Prescrizioni procedurali per i costruttori dei veicoli

I costruttori dei veicoli non consentono l'accesso alle RMI connesse alla sicurezza a meno che non siano rispettate tutte le prescrizioni procedurali indicate di seguito.

(1) Prescrizioni procedurali per i veicoli rubati

I costruttori dei veicoli tengono un registro di tutti i veicoli del proprio marchio segnalati dalle autorità come rubati.

I costruttori dei veicoli istituiscono una procedura che garantisca in maniera chiara tracciabilità e affidabilità e consenta alle autorità competenti di tracciare i dati da essi forniti ai dipendenti degli OI cui è consentito l'accesso alle informazioni relative al veicolo rubato.

(2) Prescrizioni procedurali per la conservazione delle informazioni

Per ciascun accesso consentito alle informazioni sulla riparazione e la manutenzione connesse alla sicurezza, i costruttori dei veicoli conservano le informazioni indicate di seguito:

(a) il numero di identificazione (VIN) del veicolo per il quale sono state richieste le informazioni;

(b) la data in cui è stata presentata la richiesta;

(c) il numero di immatricolazione del veicolo per il quale sono state richieste le informazioni, se disponibile;

(d) la variante del tipo di veicolo per il quale sono state richieste le informazioni e la versione di tale veicolo, se disponibile.

I costruttori dei veicoli devono conservare tali dati per un periodo di 5 anni.