Tulkojums

LATVIJAS KOMPETENTĀS INSTITŪCIJAS DIGITĀLĀ TAHOGRĀFA SISTĒMAI DARBĪBAS VADLĪNIJAS

Versiju vēsture Latvijas kompetentās institūcijas darbības digitālā tahogrāfa sistēmai

Versija	Datums	Komentāri
1.versija	2005.gada 21.jūlijā	Apstiprināta Digital Tachograph Root Certification Authority Traceability and Vulnerability Assessment Unit European Commission Joint Research Centre, Ispra Establishment
2.versija	2011.gada 26.septembrī	Autotransporta direkcija veica grozījumus sekojošos punktos: 1.1; 1.2; 1.3; 3; 11.1.
3.versija	2016.gada 7.septembrī	Autotransporta direkcija veica grozījumus sekojošos punktos: 1; 1.1; 1.2; 3.2.2; 5.1.4

Saturs

1 Ievads

Šis dokuments ir Latvijas kompetentās institūcijas digitālā tahogrāfa sistēmai nacionālās vadlīnijas.

Kompetentās institūcijas digitālā tahogrāfa sistēmai nacionālās vadlīnijas atbilst:

- Padomes 1998. gada 24. septembra Regulai (EK) Nr. 2135/98, ar ko groza Regulu (EEK) Nr.3821/85 par reģistrācijas kontrolierīcēm, ko izmanto autotransportā
- Komisijas 2002. gada 13. jūnija Regulai (EEK) Nr. 1360/2002, kas saistībā ar tehnisko progresu septīto reizi adaptē Padomes Regulu (EEK) Nr.3821/85 par reģistrācijas kontrolierīcēm, ko izmanto autotransportā
- Eiropas Parlamenta un Padomes 2014. gada 4. februāra Regulai Nr.165/2014 par tahogrāfiem autotransportā, ar kuru atceļ Padomes Regulu (EEK) Nr. 3821/85 par reģistrācijas kontrolierīcēm, ko izmanto autotransportā, un groza Eiropas Parlamenta un Padomes Regulu (EK) Nr. 561/2006, ar ko paredz dažu sociālās jomas tiesību aktu saskaņošanu saistībā ar autotransportu
- Komisijas 2016. gada 18. marta Īstenošanas Regulai (ES) 2016/799, ar ko Īsteno Eiropas Parlamenta un Padomes Regulu (ES) Nr. 165/2014, ar kuru nosaka prasības attiecībā uz tahogrāfu un to komponentu konstrukciju, testēšanu, uzstādīšanu, darbību un remontu
- Nacionālās sertifikācijas nodrošināšanas vadlīnijām, versija 1.0
- Eiropas kopējām digitālā tahogrāfa drošības vadlīnijām, versija 1.0
- Eiropas galvenās digitālā tahogrāfa sistēmas pamatnostādnes, versija 2.1

Šajā dokumentā lietoto saīsinājumu skaidrojumi atrodami šī dokumenta beigās sadaļā 14.2

1.1 Atbildīgā organizācija

Autotransporta direkcija ir dalībvalsts kompetentā institūcija (MSA), sertifikācijas institūcija (MSCA) un karšu izsniegšanas institūcija (CIA), kas atbildīga par Latvijas kompetentās institūcijas digitālā tahogrāfa sistēmai nacionālo vadlīniju ievērošanu.

Autotransporta direkcija
Vaļņu iela 30
Rīga, LV – 1050
Latvija

MSCA var noslēgt līgumu par savu tehnisko funkciju nodošanu servisa aģentūrai, kas izpilda sertifikācijas veicēja (CSP) funkciju.

CIA var noslēgt līgumu par atsevišķu ar karšu izsniegšanu saistītu funkciju nodošanu apakšlīgumslēdzējiem (servisa aģentūrām).

Servisa aģentūru iesaistīšana nemazina MSA atbildību par visu funkciju izpildi.

Servisa aģentūra, kas nodrošina CSP funkciju un kuras detalizēts darbības apraksts šīs funkcijas nodrošināšanai ir ietverts sertifikācijas veicēja darbības aprakstā (CPS), ir Trüb Baltic AS.

Trüb Baltic AS
Laki 5
10621Tallina
Igaunija

Servisa aģentūra, kas nodrošina Karšu personalizācijas veicēja (CP) funkciju un kuras detalizēts darbības apraksts šīs funkcijas nodrošināšanai ir ietverts personalizācijas veicēja darbības aprakstā (CP), ir Trüb Baltic AS.

Trüb Baltic AS
Laki 5
10621Tallina
Igaunija

1.2 Apstiprināšana

Latvijas kompetentās institūcijas digitālā tahogrāfa sistēmai nacionālās vadlīnijas ir apstiprinājusi:

Digital Tachograph European Root Certification Authority – TP 361
European Commission
Joint Research Centre
Directorate E- Space, Security & Migration
Cyber & Digital Citizens' Security Unit
Via Enrico Fermi, 2749
I-21027 Ispra (VA), Italy

2011. gada 15.oktobrī

1.3 Publicitāte un kontakti

Latvijas kompetentās institūcijas digitālā tahogrāfa sistēmai nacionālās vadlīnijas publiski pieejamas: http://www.atd.lv

Jautājumi, kas saistīti ar šīm Latvijas kompetentās institūcijas digitālā tahogrāfa sistēmai nacionālajām vadlīnijām adresējami:

Autotransporta direkcijai
Vaļņu iela 30
Rīga, LV – 1050
Latvija
tālrunis: (371) 67280485
fakss: (371) 67821107

2 Darbības sfēra un piemērojamība

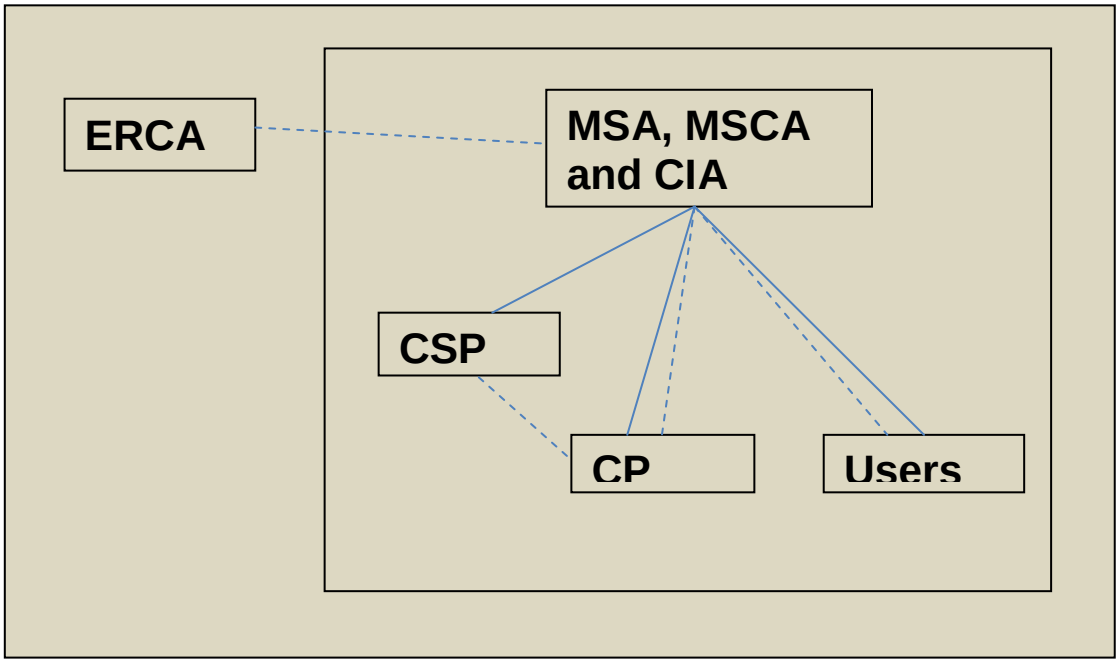
Latvijas kompetentās institūcijas digitālā tahogrāfa sistēmai nacionālās vadlīnijas attiecas tikai uz digitālā tahogrāfa sistēmu.

MSCA ģenerētie kodi un sertifikāti izmantojami tikai digitālā tahogrāfa sistēmas ietvaros.

CIA izsniegtās kartes izmantojamas tikai digitālā tahogrāfa sistēmas ietvaros.

3 Vispārīgie nosacījumi

Šajā nodaļā ietverts MSA, CIA, MSCA, CSP, CP, servisa aģentūru un lietotāju pienākumu uzskaitījums un citi ar normatīviem aktiem un strīdu izskatīšanas kārtību saistīti jautājumi.



Ar Nacionālo digitālā tahogrāfa sistēmu saistīto savstarpējo attiecību hierarhija un datu apmaiņa

Attēlā lietotie saīsinājumi un simboli:

ERCA	Eiropas Galvenā sertifikācijas institūcija
MSA	Dalībvalsts kompetentā institūcija
MSCA	Dalībvalsts sertifikācijas institūcija
CSP	Sertifikācijas veicējs
CIA	Karšu izsniegšanas institūcija
CP	Karšu personalizācijas veicējs
_____	Atbildības hierarhija
_ _ _ _ _ _ _ _	Datu un informācijas plūsmas vai karšu izsniegšanas kārtība

Pārējie saīsinājumi atrodami apakšpunktā 14.2

3.1 Pienākumi

Šajā apakšnodaļā ietverts pienākumu uzskatījums:

- MSA
- MSCA
- CIA
- CSP
- CP
- Servisa aģentūrām
- Karšu īpašniekiem vai lietotājiem

3.1.1 MSA pienākumi

Saistībā ar šīm Latvijas kompetentās institūcijas digitālā tahogrāfa sistēmai nacionālām vadlīnijām MSA ir šādi pienākumi:

a) nodrošināt atbilstību šīm nacionālajām vadlīnijām;

b) nozīmēt MSCA un CIA;

c) veikt MSCA, CIA, CSP, CP, ieskaitot servisa aģentūras, darbības auditu;

d) informēt par šīm vadlīnijām iesaistītās puses un servisa aģentūras;

e) nodrošināt, ka šīs vadlīnijas apstiprina ERCA.

3.1.2 MSCA pienākumi

MSCA pienākums ir :

a) ievērot šīs Latvijas kompetentās institūcijas digitālā tahogrāfa sistēmai nacionālās vadlīnijas;

b) publicēt CPS, kurā ietverta atsauce uz šīm nacionālajām vadlīnijām un ko apstiprinājusi MSA;

c) nodrošināt, ka, veicot sertifikāciju, tiek ievērotas ERCA galveno digitālā tahogrāfa sistēmas pamatnostādņu prasības;

d) nodrošināt pietiekamus funkcionālos un finanšu resursus, lai darbotos atbilstoši nacionālo vadlīniju prasībām, jo īpaši, ņemot vērā apakšpunktā 3.2 minēto atbildības risku.

MSCA nodrošina, ka visas šajās vadlīnijās MSCA izvirzītās prasības tiek izpildītas.

MSCA ir atbildīga par funkciju veikšanu šajās vadlīnijās noteiktajā kārtībā arī tad, ja noslēgts līgums par tehnisko funkciju nodošanu servisa aģentūrai, kas izpilda sertifikācijas veicēja (CSP) funkciju. MSCA ir atbildīga par to, lai servisa aģentūra sniegtu pakalpojumus atbilstoši sertifikācijas veicēja darbības aprakstam (CPS) un nacionālajām MSA vadlīnijām.

3.1.3 CIA pienākumi

CIA pienākums ir:

a) ievērot šīs Latvijas kompetentās institūcijas digitālā tahogrāfa sistēmai nacionālās vadlīnijas;

b) publicēt CP PS, kurā ietverta atsauce uz šīm nacionālajām vadlīnijām un kuru apstiprinājusi MSA;

c) nodrošināt, ka, pasūtot karti, CP par klientu tiek sniegta pareiza un visa nepieciešamā informācija;

d) informēt karšu lietotājus par šajās vadlīnijās ietvertajām ar sistēmu saistītajām prasībām;

e) nodrošināt pietiekamus funkcionālos un finanšu resursus, lai darbotos atbilstoši nacionālo vadlīniju prasībām, jo īpaši, ņemot vērā apakšpunktā 3.2 minēto atbildības risku

3.1. 4 CSP pienākumi

CSP pienākums ir:
a) nodrošināt, ka CP nodotie sertifikāti ir pareizi;

b) nodrošināt MSCA privātā koda slepenību;

c) ievērot šīs Latvijas kompetentās institūcijas digitālā tahogrāfa sistēmai nacionālās vadlīnijas;

d) nodrošināt pietiekamus funkcionālos un finanšu resursus, lai darbotos atbilstoši nacionālo vadlīniju prasībām, jo īpaši, ņemot vērā apakšpunktā 3.2 minēto atbildības risku

3.1. 5 CP pienākumi

Izraudzītā CP pienākums ir:

a) ievērot šīs Latvijas kompetentās institūcijas digitālā tahogrāfa sistēmai nacionālās vadlīnijas;

b) nodrošināt, ka tiek izpildītas visas tam šajās vadlīnijās izvirzītās prasības.

CP ir atbildīgs par to, lai arī tad, ja daļa funkciju ar apakšlīguma starpniecību tiek nodotas servisa aģentūrai, procedūra atbilstu šajās vadlīnijās noteiktajai kārtībai.

3.1.6. Servisa aģentūras pienākumi

Servisa aģentūru, kas sniedz ar šīm vadlīnijām saistītus pakalpojumus, saistību apjoms pret MSA, MSCA un CIA tiek noteikts savstarpējos līgumos. Neskatoties uz šādiem līgumiem, MSA ir pilnībā atbildīga par jebkuru šajā dokumentā ietvertu un ar digitāliem tahogrāfiem saistītu pakalpojumu izpildi.

3.1.7. Karšu lietotāju pienākumi

CIA nodrošina, ka, parakstot vienošanos ar lietotāju (skatīt 5.1.2.2), lietotājs (vai lietotāja organizācija) izpilda šādas prasības:

3.1.7.1 Visi karšu veidi

a) iesniedz CIA precīzu un pilnīgu informāciju saskaņā ar šo vadlīniju prasībām, īpaši saistībā ar reģistrāciju;

b) kodus un sertifikātus izmanto tikai digitālā tahogrāfa sistēmā;

c) karti izmanto tikai digitālā tahogrāfa sistēmā;

d) rūpējas, lai nevarētu notikt nesankcionēta ierīces privātā koda un kartes izmantošana;

e) lietotājam tikai īpašos un pamatotos gadījumos var būt gan darbnīcas, gan uzņēmuma karte;

f) nelieto bojātu karti vai tādu, kurai beidzies derīguma termiņš;

g) nekādā veidā nemaina vai nemēģina izmainīt karti;

h) lietotājs nekavējoties informē CIA, ja norādītajā sertifikāta derīguma termiņā iestājas viens no tālāk minētajiem gadījumiem:

- ierīces privātais kods vai karte ir nozaudēta, nozagta vai iespējams nesankcionēti lietota; vai
- sertifikāta saturs ir vai būs nepareizs.

3.1.7.2 Vadītāja karte

a) lietotājam var būt tikai viena derīga vadītāja karte;
b) lietotājs var izmantot tikai savus kodus, sertifikātu un karti.

3.1.7.3 Darbnīcas karte

a) lietotājam jārūpējas par sava PIN koda drošību;

b) karte nedrīkst iznest ārpus darbnīcas telpām, izņemot gadījumus, ja tas saistīts ar tahogrāfu uzstādīšanu, kalibrāciju un remontu.

3.1.8 VU ražotāju pienākumi (darbojoties kā personalizācijas veicējam)

Pašlaik un arī tuvākajā nākotnē uz Latviju nav attiecināms.

3.1.9 Kustības sensoru ražotāju pienākumi (darbojoties kā personalizācijas veicējam)

Pašlaik un arī tuvākajā nākotnē uz Latviju nav attiecināms.

3.2 Atbildība

3.2.1 MSCA, CPS, CP un atbildība pret MSA un CIA

MSCA, CPS, CP ir atbildīgi par tiem uzticēto uzdevumu pilnīgu izpildi arī tad, ja daļa no šiem uzdevumiem tiek nodoti izpildei Servisa aģentūr;am. Ja MSCA vai CIA plāno slēgt līgumu par atsevišķu funkciju nodošanu citām pusēm, tiem par šādu nodomu pirms līguma noslēgšanas jāinformē MSA.

MSCA un CIA ir atbildīgi par zaudējumiem, kas radušies pienākumu neizpildes rezultātā, tikai tad, ja tie ir rīkojušies nolaidīgi. Ja iestāde ir rīkojusies saskaņā ar šīm MSA vadlīnijām un attiecīgo PS, tad tāda rīcība par nolaidīgu nav uzskatāma.

MSCA, CSP, CP nekādā mērā nav atbildība attiecībā pret galalietotājiem. Tie ir atbildīgi tikai attiecībā pret MSA un CIA.

Visa veida atbildība pret galalietotājiem ietilpst attiecīgi MSA vai CIA kompetencē.

3.2.2 MSA un CIA atbildība pret galalietotājiem un iesaistītajām pusēm

MSA ir atbildīga par pareizu Regulas (EEK) Nr.3821/85, ko groza ar Padomes Regulu (EK) Nr. 2135/98 un tās pielikumu IB, un Regulas (EU) Nr. 165/2014 piemērošanu. Tas nozīmē, ka MSA īpaši atbildīga par to, lai nodrošinātu, ka:

a) sertifikāts veidots saskaņā ar Regulas un šo MSA vadlīniju prasībām;

b) sertifikātā izdošanas brīdī tajā ir ietverta visa digitālā tahogrāfa sertifikātam nepieciešamā informācija, jo īpaši, tas, lai dati par kartes īpašnieku atbilstu tai informācijai, kas sniegta iesniegumā.

CIA ir atbildīga par to, lai tiktu veikta sertifikātā ietverto kartes īpašnieka datu un attiecīgajā iesniegumā sniegtās informācijas salīdzināšana.

MSA vai CIA nav atbildīga par zaudējumiem galalietotājiem un iesaistītajām pusēm, ja šie zaudējumi radušies:

1) nepatiesas vai nepilnīgas iesniedzēja sniegtās informācijas dēļ; izņemot gadījumus, ja pierādīts, ka MSA vai CIA rīkojusies nolaidīgi.;

2) sertifikātu izmantošanas citiem mērķiem, kā noteikts Regulā, dēļ;

3) jo atklātībā nonācis PIN kods, izņemot gadījumus, ja tas noticis MSA vai CIA vainas dēļ;

4) VU vai telekomunikācijas sakaru bojājumu vai līdzīga iemesla, kas rada sertifikāta izmantošanas Tahogrāfu sistēmā traucējumus, dēļ.

MSA vai CIA nekad nav atbildīgi par netiešiem finansiāliem vai cita veida netiešiem zaudējumiem galalietotājiem, iesaistītajām pusēm vai pusēm, ar ko tās noslēgušas līgumus.

Turklāt, digitālā tahogrāfa kartes, kodi un sertifikāti paredzēti izmantošanai tikai Tahogrāfu sistēmā. Jebkādi citi sertifikāti saistībā ar digitālā tahogrāfa karti ir pretrunā ar šīm vadlīnijām, un par šādiem pārkāpumiem ne MSA, ne CIA nav atbildīgi.

3.2.3 Noteicošie normatīvie akti

Atbildība par radītajiem zaudējumiem nosakāma Latvijas Administratīvā procesa likuma noteiktajā kārtībā (publicēts: Latvijas Vēstnesis 14.11.2001).

3.3 Interpretācija un prasību izpilde

3.3.1 Noteicošā likumdošana

Šo vadlīniju prasības interpretējamas atbilstoši Latvijas likumdošanai.

3.4 Konfidencialitāte

Konfidencialitātes nosacījums ievērojams saskaņā ar direktīvu 95/46/EK un Fizisko personu datu aizsardzības likumu (publicēts: Latvijas Vēstnesis 06.04.2000).

3.4.1 Konfidenciāli glabājama informācija

Jebkura veida informācija par fiziskām vai juridiskām personām, kas nonāk MSCA, CSP, CIA vai servisa aģentūru rīcībā un neparādās uz izdotajām kartēm vai sertifikātiem, uzskatāma par konfidenciālu un nav izplatāma bez kartes lietotāja vai (attiecīgajos gadījumos) bez lietotāja darba devēja vai tā pārstāvja iepriekšējas piekrišanas, izņemot gadījumus, ja normatīvos aktos noteikts citādi.

Visi privātie un slepenie kodi, ko MSCA vai CP lieto savu funkciju izpildei šo nacionālo MSA vadlīniju ietvaros, glabājama konfidenciāli.

Audita dokumenti un slēdzieni, izņemot normatīvos aktos noteiktos gadījumus, nav pilnībā publiskojami

3.4.2 Informācija, kas nav uzskatāma par konfidenciālu

Sertifikāti nav uzskatāmi par konfidenciāliem.

Identifikācijas dati un cita veida informācija par fiziskām vai juridiskām personām, kas parādās uz kartēm un sertifikātos, nav uzskatāma par konfidenciālu, izņemot gadījumus, ja to nosaka normatīvie akti vai speciāli līgumi.

4. Darbības apraksts (PS)

MSCA, CIA, CSP, CP ir jābūt darbības aprakstam (PS), kurā ietvertas visas darbības un procedūras, lai nodrošinātu šajās nacionālajās MSA vadlīnijās noteikto prasību izpildi. MSA šādi PS jāapstiprina.

Jo īpaši:

a) PS jānosaka visu to iesaistīto organizāciju, kas nodrošina pakalpojumus saistībā ar MSCA un CIA funkcijām, pienākumi, ieskaitot piemērojamās darbības shēmas un procedūras;

b) PS jānosūta MSA, digitālā tahogrāfa sistēmas lietotājiem un iesaistītajām pusēm, piemēram, kontroles institūcijām;

   Tomēr, pilnīgi viss darbības apraksts MSCA/CIA nav lietotājiem jāpublisko.

c) MSCA/CIA vadība ir atbildīga par to, lai PS tiktu pilnībā ievērots;

d) MSCA/CIA jānosaka PS izvērtēšanas procedūra;

e) MSCA, CIA, CSP, CP savlaicīgi jāziņo par grozījumiem, ko tās plāno PS izdarīt, un pēc attiecīgo grozījumu apstiprināšanas grozītais PS nekavējoties jānosūta iesaistītajām pusēm.

5. Ierīces administrēšana

Tahogrāfa sistēmas ierīce sastāv no:

- tahogrāfa kartes;
- transportlīdzekļa reģistrācijas ierīces bloka;
- kustības sensoriem.

Ņemot vērā, ka reģistrācijas ierīces blokus un kustības sensorus Latvijā neražo, šajā vadlīniju nodaļā iekļautas tikai tahogrāfu kartes.

Ierīces darbības nodrošināšanā ir iesaistītas vairākas puses:

- CIA (karšu anulēšana, karšu reģistrācija, atjaunošana, u.c.);
- MSCA (kustības sensoru kodi);
- CP (vizuālā un elektroniskā personalizācija, kodi);
- CSP (sertifikāti).

MSA veic šādas funkcijas:

- kvalitātes kontrole (tipa apstiprinājums). Faktisko darbu veiks servisa aģentūra, kas izraudzīta veikt CP funkciju;
- darbības aprakstu apstiprināšana.

CIA veic šādas funkcijas:

- iesniegumu karšu izsniegšanai pieņemšana;
- apstiprināto iesniegumu reģistrācija;
- CP nodrošināšana ar personalizācijai nepieciešamajiem datiem;
- datu glabāšana (DB);
- informācijas apmaiņa ar citām dalībvalstīm;
- lietotāju reģistrācija;
- karšu izsniegšana lietotājiem;
- pazaudēto un atrasto karšu uzskaite;

MSCA veic šādas funkcijas:

- MSCA kodu ģenerēšana Latvijai un saiknes ar ERCA sertifikācijas procesu nodrošināšana.

CSP veic šādas funkcijas:

- karšu sertifikātu ģenerēšana pēc CP pasūtījuma;
- izsniegto sertifikātu ievadīšana DB;
- MSCA kodu drošas glabāšanas nodrošināšana.

CP veic šādas funkcijas:

- kvalitātes kontrole (karšu paraugu testēšana);
- sertifikātu pieprasījumu nosūtīšana CSP;
- kodu un sertifikātu ievietošana;
- karšu personalizācija;
- nepieciešamības gadījumā karšu funkcionalitātes pārbaude;
- karšu piegāde CIA

- darbnīcas karšu un PIN kodu piegāde CIA.

5.1 Tahogrāfa kartes

5.1.1 Kvalitātes kontrole – MSA/CP funkcija

MSA/CP nodrošina, ka tikai kartes, kurām ir tipa apstiprinājums atbilstoši Regulas nosacījumiem, tiek personalizētas

5.1.2 Iesniegums karšu saņemšanai –CIA funkcija

CIA informē lietotājus par kartes izmantošanas noteikumiem. Šai informācijai jābūt pieejamai vismaz latviski un angliski.

Lietotājam, iesniedzot iesniegumu kartes saņemšanai un pēc tam saņemot karti, ir jāapņemas šos karšu izmantošanas noteikumus ievērot.

5.1.2.1 Lietotāju iesniegumi

Tahogrāfa karšu pieprasītājiem ir jāiesniedz iesniegums formā, ko nosaka CIA. Iesniegumā vismaz jābūt norādītiem datiem, kas nekļūdīgi ļauj identificēt lietotāju. Iesniedzot iesniegumu uzņēmuma, darbnīcas un kontroles kartes saņemšanai, jāiekļauj dati par attiecīgo juridisko personu, kurai karti lūgts izsniegt.

Lai izsniegtu karti nepieciešama tālāk minētā informācija. Ja vien to nav iespējams iegūt no citiem avotiem, tā iekļaujama iesniegumā:

Vadītāja kartei:

- vārds, uzvārds
- dzimšanas datums un vieta
- pastāvīgās dzīvesvietas adrese
- personas kods (ja tāds ir)
- pasta adrese
- fotogrāfija
- vadītāja apliecības numurs

Darbnīcas kartei:

Darbnīcas karte izsniedzama tikai fiziskām personām, kuras ir darba attiecībās ar attiecīgu juridisku personu un kuras sniegušas šādas ziņas:

- juridiskās personas, ar kuru ir darba attiecības, vai citas organizatoriskās formas nosaukums un juridiskais statuss;

- informācija par kartes lietotāju (ieskaitot vārdu(us), uzvārdu, personas kodu un fotogrāfiju)

Kontroles kartei:

Kontroles karte izsniedzama tikai fiziskām personām, kuras ir darba attiecībās ar attiecīgu juridisku personu un kuras sniegušas šādas ziņas

- juridiskās personas, ar kuru ir darba attiecības, vai citas organizatoriskās formas nosaukums un juridiskais statuss;

- fakultatīvi informācija par kartes lietotāju un fotogrāfija (ieskaitot vārdu(us), uzvārdu, personas kodu), obligāti kontroles vienības nosaukums;

Uzņēmuma kartei:

Uzņēmuma karte izsniedzama tikai to uzņēmumu pārstāvjiem, kuru uzņēmumā ir ar digitāliem tahogrāfiem aprīkoti transportlīdzekļi un kuri snieguši šādas ziņas:

- attiecīgās juridiskās personas vai citas organizatoriskās formas nosaukums un juridiskais statuss;

- informācija par attiecīgās juridiskās personas vai citas organizatoriskās formas reģistrāciju (piemēram, Uzņēmumu reģistrā);

- kartes lietotāja saistība ar attiecīgo juridisko personu vai citu organizatorisko formu;

- fakultatīvi informācija par kartes lietotāju (ieskaitot vārdu(us), uzvārdu, personas kodu).

5.1.2.2 Vienošanās

Iesniedzējam, kas iesniedzis iesniegumu kartes saņemšanai un apliecinājis, ka karti saņēmis, jānoslēdz vienošanās ar CIA, kurā ietverti vismaz šādi nosacījumi:

- lietotājs piekrīt ievērot tahogrāfa kartes izmantošanas nosacījumus;
- lietotājs piekrīt un apliecina, ka, sākot no kartes derīguma termiņa sākuma brīža un visā tās derīguma laikā, kamēr lietotājs nav sniedzis CIA nekādu citu informāciju,: :
    - rūpēsies, lai kartei nepiekļūtu nesankcionētas personas;
    - visa lietotāja CIA sniegtā informācija kartes izsniegšanai ir patiesa;
    - karte tiks apzinīgi lietota, ievērojot visus attiecīgai kartei noteiktos lietošanas ierobežojumus.

5.1.2.3 CIA nosacījumi iesnieguma apstiprināšanai - Vadītāja kartei

Vadītāja karte izsniedzama tikai tām fiziskām personām, kuras pastāvīgi dzīvo iesnieguma iesniegšanas valstī.

CIA jāpārliecinās, ka iesniedzējam nav derīga vadītāja karte, kas izsniegta Latvijā vai citā dalībvalstī.

CIA jāpārliecinās, ka iesnieguma vadītāja kartes saņemšanai iesniedzējam ir derīga attiecīgās kategorijas vadītāja apliecība.

5.1.2.4 CIA nosacījumi iesnieguma apstiprināšanai – Darbnīcas kartei

Darbnīcas karte izsniedzama tikai tām darbnīcām, kurām ir spēkā esoša akreditācija darbībām ar digitālo tahogrāfu.

5.1.2.5 CIA nosacījumi iesnieguma apstiprināšanai – Kontroles kartei

Kontroles karte izsniedzama tikai tām institūcijām, kurām oficiāli kontroles funkcija deleģēta.

5.1.2.6 CIA nosacījumi iesnieguma apstiprināšanai – Uzņēmuma kartei

Uzņēmuma karte izsniedzama tikai tiem uzņēmumiem, kas reģistrēti atbilstoši nacionālās likumdošanas prasībām.

5.1.3 Karšu derīguma termiņš

Darbnīcas kartes drīkst būt derīgas ne ilgāk kā **vienu** gadu no to izsniegšanas dienas.

Vadītāja kartes drīkst būt derīgas ne ilgāk kā **piecus** gadus no to izsniegšanas

Uzņēmuma kartes drīkst būt derīgas ne ilgāk kā **piecus** gadus no to izsniegšanas dienas.

Kontroles kartes drīkst būt derīgas ne ilgāk kā **divus** gadus no to izsniegšanas dienas.

CIA izstrādā procedūru, kā lietotājiem atgādināt, ka tuvojas beigām kartes derīguma termiņš.

Iesnieguma kartes atjaunošanai gadījumā ievēro sadaļā 5.1.2 aprakstītās prasības.

5.1.4 Karšu atjaunošana –CIA funkcija

Lietotājs iesniedz iesniegumu kartes atjaunošanai vismaz **15** darba dienas pirms kartes derīguma termiņa beigām.

Ja lietotājs ievēro iepriekšējā rindkopā minēto nosacījumu, CIA izsniedz jaunu karti pirms darbībā esošās kartes termiņa beigām.

5.1.5 Kartes nomaiņa – CIA funkcija

Lietotājs, kurš pārceļas dzīvot uz citu valsti, var pieprasīt, lai viņam piederošo vadītāja karti nomaina. Ja esošā karte ir derīga, lietotājam iesnieguma apstiprināšanai jāiesniedz tikai pierādījums, ka Latvija ir viņa pastāvīgā dzīves vieta.

CIA, izsniedzot jaunu karti, pieprasa nodot iepriekšējo, kuru nosūta šīs kartes izdevējvalsts MSA.

Karšu nomaiņai dzīves vietas maiņas dēļ piemērojama jaunas kartes izsniegšanas procedūra (sadaļa 5.1.2).

5.1.6 Nozaudētu, nozagtu, bojātu un nefunkcionējošu karšu nomaiņa – CIA funkcija

Ja karte nozaudēta vai nozagta, lietotājs par to informē CIA.

Informācija par nozagtajām un pazaudētajām ievietojama melnajā sarakstā, kas pieejams visu dalībvalstu institūcijām.

Bojātas un nefunkcionējošas kartes nododamas CIA, kas tās izsniegusi un kura tās vizuāli un elektroniski anulē un iekļauj melnajā sarakstā.

Ja karte nozaudēta, nozagta, bojāta vai nefunkcionē, lietotājam jāiesniedz iesniegums kartes nomaiņai **7** dienu laikā.

Ja lietotājs ievēro iepriekšējā rindkopā minēto prasību, tad CIA jānomaina karte ar jaunu kodu un sertifikātu **5** darba dienu laikā, skaitot no iesnieguma kopā ar visiem nepieciešamajiem dokumentiem iesniegšanas dienas.

Nomainītajai kartei jābūt tādam pašam derīguma termiņam kā iepriekšējai. Ja nomainot kartes derīguma termiņš ir īsāks par trim mēnešiem, CIA var karti nevis nomainīt, bet atjaunot.

5.1.7 Apstiprinātu iesniegumu reģistrācija – CIA funkcija

CIA apstiprināto iesniegumu datus ievada datu bāzē. Pēc tam šos datus nosūta CP, kas sniegto informāciju izmanto sertifikātu ģenerēšanas un karšu personalizācijas procesā.

5.1.8 Karšu personalizācija –CP funkcija

Kartes tiek personalizētas gan vizuāli, gan elektroniski. Ja šo procesu veic servisa aģentūra (CP), tas nemazina MSA atbildību par visu procesu.

5.1.8.1 Vizuālā personalizācija

Kartes vizuāli personalizējamas saskaņā ar Regulas pielikuma 1B sadaļu IV [REG-A].

- Uz vadītāja un darbnīcas kartes jābūt kartes lietotāja fotogrāfijai.

5.1.8.2 Datu par lietotāju ievadīšana

Dati kartē ievadāmi kārtībā, kas norādīta Regulas 1360/2002 pielikuma 1B 2. papildinājuma [REG-A] noteikumos TCS_403, TCS_408, TCS_413 un TCS_418 atkarībā no kartes veida.

5.1.8.3 Kodu ievadīšana

Privātais kods ievadāms kartē tā, lai tas vienmēr atrastos tikai šī koda ģenerēšanas vidē. Šajā vidē jānodrošina apstākļi, ka neviens nekādā veidā bez identifikācijas ģenerēto privāto kodu uzzināt nevar. Ieteicams kodus ģenerēt vai nu kartē, vai HSM. Skatīt arī sadaļu 7.2 par ierīces kodu administrēšanu.

5.1.8.4 Sertifikāta ievadīšana

Lietotāja sertifikāts ievadāms kartē pirms to izsniedz lietotājam.

5.1.8.5 Kvalitātes kontrole

Jābūt izstrādātai procedūrai, kas nodrošina, ka vizuālā informācija uz kartes un elektroniski ievadītā informācija un sertifikāti savstarpēji atbilst, kā arī tā atbilst informācijai, ko par sevi sniedzis potenciālais kartes īpašnieks. Šai procedūrai jābūt aprakstītai CP PS.

5.1.8.6 Neizsniegtu karšu anulēšana (iznīcināšana)

Visas kartes, kas personalizācijas procesā sabojātas vai salūzušas (vai cita iemesla dēļ nav izgatavotas un nosūtītas) fiziski un elektroniski iznīcināmas.

5.1.9 Karšu reģistrācija un datu uzglabāšana (DB) – CP un CIA funkcija

CP un CIA ir atbildīgas par to, lai tiktu reģistrēts, kura karte un ar kuru numuru lietotājam izsniegta. CP pārsūta attiecīgos datus uzglabāšanai CIA datu bāzē.

5.1.10 Karšu izsniegšana lietotājiem – CP un CIA funkcija

a) Personalizācija plānojama tā, lai pēc iespējas samazinātu laiku, kad karti līdz izsniegšanai nepieciešams droši glabāt. Ārpus darba laika nepieciešams nodrošināt glabāšanu seifā. Jāizstrādā instrukcija rīcībai ārkārtas situācijās, ieskaitot pārtraukumus ražošanā, piegādes aizkavēšanos, karšu pazaudēšanu vai sabojāšanos.
b) Personalizētās kartes nekavējoties jānogādā norādītajā piegādes vai izsniegšanas vietā, tas ir, vietā, kas tiek uzraudzīta.
c) Personalizētās kartes vienmēr jāglabā atsevišķi no nepersonalizētām kartēm.
d) Tahogrāfa karšu izsniegšana jāorganizē tādā veidā, lai samazinātu karšu nozaudēšanas risku.
e) Gadījumos, kad karte izsniedzama lietotājam, kura identitāte, iesniedzot iesniegumu nav pārbaudīta, izsniegšanas vietā jāpārbauda vai lietotāja identitātes dati (piemēram, vārds, uzvārds) atbilst tās fiziskās personas datiem, kas ieradusies.
f) Lietotājam jāuzrāda derīgs identifikācijas dokuments.
g) Saņemot karti, tās lietotājs parakstās.

5.1.11 Kodu autentifikācija (PIN) –ģenerē CP

Šī sadaļa attiecas tikai uz darbnīcas kartēm.
Darbnīcas kartēm jābūt PIN kodam, kas nepieciešams, lai karti autentificētu transportlīdzekļa reģistrācijas ierīces blokā (Regulas pielikums 1B, 10.papildinājums [REG-A]: Tahogrāfa kartes: 4.2.2)

PIN kods sastāv vismaz no **4** cipariem (Regulas pielikums 1B, 10. papildinājums [REG-A]: transportlīdzekļa reģistrācijas ierīces bloks: 4.1.2).

5.1.10.1 PIN koda ģenerēšana

PIN kodi ģenerējami drošā sistēmā, kas pēc tam drošā vidē pārvietojami darbnīcas kartēs un uzreiz iedrukājami PIN aploksnēs. Tā, ka var identificēt saikni starp PIN un lietotāju, PIN kodus datorsistēmā uzglabāt nedrīkst. PIN kodu ģenerēšanas sistēmai jāatbilst ITSEC E3, CC EAL4 vai ekvivalentām drošības kritēriju prasībām.

5.1.10.2 PIN kodu nosūtīšana

PIN kodus var nosūtīt pa pastu.

PIN kodi nevar būt vienā sūtījumā kopā ar attiecīgo karti.

5.1.12 Kartes deaktivizācija –CIA un CP funkcija

Jābūt iespējai karti un ar to saistītos kodus pavisam deaktivizēt. Lēmumu par deaktivizāciju pieņem CIA; faktiski to veic vai nu CIA, vai CP.

Karšu deaktivizācija veicama, izmantojot tam piemērotu ierīci. Pēc tam jāpārliecinās, ka kartes un kodu funkcionēšana tiešām pārtraukta. Karte anulējama arī vizuāli.

Karšu deaktivizācija reģistrējama karšu datu bāzē un kartes numurs iekļaujams melnajā sarakstā.

5.2 Transportlīdzekļa reģistrācijas ierīces bloki un kustības sensori

Pašlaik un arī tuvākajā nākotnē uz Latviju nav attiecināms, izņemot gadījumus, kad transportlīdzekļa reģistrācijas ierīces bloks bojāts vai nefunkcionē. Ja iespējams, darbnīcai dati no transportlīdzekļa reģistrācijas ierīces bloka lejupjāielādē un jānodod attiecīgajam uzņēmumam. Ja to izdarīt nav iespējams, darbnīcai par to uzņēmumam jāsagatavo ziņojums.

6 Kodu administrēšana: Eiropas publiskais kods, dalībvalstu kodi, kustības sensoru kodi

Šajā sadaļā iekļauti nosacījumi šādu kodu administrēšanai:

- Eiropas publiskais kods - ERCA publiskais kods;
- dalībvalstu kodi, tas ir, dalībvalsts paraksta koda pāris (i);
- kustības sensoru kodi.

ERCA publiskais kods tiek izmantots, lai pārbaudītu dalībvalsts sertifikātus. ERCA privātais kods šajā sadaļā nav iekļauts, jo tas atrodas tikai un vienīgi ERCA.

Dalībvalsts kodi ir dalībvalsts paraksta kodi un tos var uzskatīt arī par dalībvalsts publiskajiem kodiem.

Kustības sensoru kodi ir simetriski kodi, kas ievietojami darbnīcas kartē, VU un kustības sensorā, lai tie savstarpēji tos atpazītu. MSCA saņem kustības sensora kodus ERCA, glabā tos un nodod CP.

Transportēšanas kodi ir asimetrisks kodu pāris, kas izmantojams, lai nodrošinātu drošu kustības sensora kodu pārvietošanu starp ERCA un MSCA.

Ja MSCA nepieciešami kādi citi kriptogrāfiski kodi, kas iepriekšējās rindkopās nav minēti, tad tie nav uzskatāmi par digitālā tahogrāfa sistēmas un šo vadlīniju sastāvdaļu.

Dalībvalsts kodi un transportēšanas kodi tiek ģenerēti un glabāti drošā un apsargātā vietā, kas nepārtraukti tiek kontrolēta un novērota. Visām ieejām ir elektroniskas atslēgas. Telpās jābūt video novērošanas sistēmai.

6.1 ERCA publiskais kods

MSCA glabā ERCA publisko kodu (EUR.PK) tā, lai saglabātu nepārtrauktu tā integritāti un pieejamību. Ja EUR.PK glabā CSP, tad uz to attiecināmi tieši tādi paši noteikumi.

CP nodrošina, ka EUR.PK tiek ievietots visās tahogrāfa kartēs un transportlīdzekļa reģistrācijas ierīces blokos.

6.2 Dalībvalsts kods

Dalībvalsts kodi ir MSCA paraksta kodu pāris(i), kas izmantojams, lai parakstītu visus tahogrāfa karšu sertifikātus. MSCA transportlīdzekļa reģistrācijas ierīču bloku sertifikātus neražo.

Kodu pāris sastāv no publiskā koda (MS.PK) un privātā koda (MS.SK).

MSCA publisko kodu sertificē ERCA, bet to vienmēr ģenerē pati MSCA.

Dalībvalstu kodus nedrīkst izmantot nekādiem citiem mērķiem kā tikai:

a) digitālā tahogrāfa karšu sertifikātu parakstīšanai;

b) pieprasījuma ERCA kodu sertifikācijai parakstīšanai, KCR, kā aprakstīts pielikumā A [ERCA]

6.2.1 Dalībvalsts kodu ģenerēšana

Dalībvalsts kodu pāra ģenerēšana veicama HSM, kas vai nu:

- atbilst prasībām, kas noteiktas FIPS 140-2 (vai 140-1) 3. līmenis vai arī augstāks [FIPS]; vai

- atbilst prasībām, kas noteiktas CEN Darbnīcu vienošanās dokumentā 14167-2 [CEN]; vai

- ir droša sistēma, kas atbilst EAL 4 vai augstākam standartam saskaņā ar ISO 15408 [CC] vai E3 vai augstākam standartam ITSEC, vai ekvivalentiem drošības kritērijiem. Tam jābūt ar tādu drošības un aizsardzības pakāpi, kas atbilst šo vadlīniju prasībām un izstrādāts balstoties uz riska analīzi un ņemot vērā praktiskos un ar tehniku nesaistītus drošības pasākumus.

Izmantotajai ierīcei un atbilstībai drošības prasībām jābūt aprakstītām CPS.

MSCA kodu pāra ģenerēšanā aktīvi jābūt iesaistītām vismaz trim personām, kuras ir atbildīgas personas MSCA vai CSP. Vismaz vienai no šīm personām jāpārstāv CA, kas atbildīga par MSCA darbību.

Kodi ģenerējami, izmantojot RSA algoritmu ar moduli koda garumam n=1024 biti (Regulas pielikums1B, papild. 11:2.1/3.2).

Lai nodrošinātu darbības nepārtrauktību, MSCA ir jābūt vairāk kā vienam dalībvalsts kodu pārim kopā ar attiecīgajiem parakstīšanas sertifikātiem.

6.2.2 Dalībvalsts kodu derīguma termiņš

Dalībvalsts privātā koda derīguma termiņš nevar pārsniegt **2** gadus, skaitot no attiecīgā publiskā koda sertifikāta izsniegšanas datuma, un pēc derīguma termiņa beigām tas nav izmantojams.

Tā kā ERCA parakstīšanas procedūras ietvaros tiek piešķirti vairāki kodu pāri, tad publiskais kods ir beztermiņa. Faktisko dalībvalsts kodu sertifikātu derīguma termiņu nosaka saskaņā ar ERCA pamatnostādnēm.

6.2.3 Dalībvalsts privātā koda glabāšana

Privātie kodi uzglabājami un izmantojami speciālā pret viltošanu drošā ierīcē (HSM), kas:

- atbilst prasībām, kas noteiktas FIPS 140-2 (vai 140-1) 3. līmenis vai arī augstāks [FIPS]; vai

- ir droša sistēma, kas atbilst EAL 4 vai augstākam standartam saskaņā ar ISO 15408 [CC] vai E3 vai augstākam standartam ITSEC, vai ekvivalentiem drošības kritērijiem. Tam jābūt ar tādu drošības un aizsardzības pakāpi, kas atbilst šo vadlīniju prasībām un izstrādāts balstoties uz riska analīzi un ņemot vērā praktiskos un ar tehniku nesaistītus drošības pasākumus.

Pieejai MSCA privātiem parakstīšanās kodiem nepieciešama dubultkontrole. Tas nozīmē, ka nevienai atsevišķai personai nevar būt zināmas visas paroles, lai piekļūtu vietai, kur glabā privāto kodu. Bet tas nenozīmē, ka, veicot ierīces sertifikātu parakstīšanu, vienmēr jābūt dubultkontrolei.

6.2.4 Dalībvalsts privātā koda dublēšana

Dalībvalsts privātos parakstīšanas kodus var dublēt, izmantojot kodu atjaunošanas procedūru, kurai nepieciešama vismaz dubultkontrole. Izmantojamā procedūra jāapraksta CPS. Dublēt privātos parakstīšanas kodus atļauts kriptētā formātā. Lai atšifrētu, nepieciešams HSM, vismaz dubultkontrole un atbilstība sadaļas 6.2.3 nosacījumiem. Tomēr, ja MSCA ir vairāki kodu pāri, kā minēts sadaļā 6.2.1, tad dublēšana nav nepieciešama.

6.2.5 Dalībvalsts privātā koda reģenerācija

Dalībvalsts privātos parakstīšanas kodus reģenerēt nedrīkst.

6.2.6 Dalībvalsts kodu uzlaušana

Jābūt rakstiskai instrukcijai, kas ietverta CPS un kurā minēti pasākumi, kas veicami lietotājiem un MSCA un/vai servisa aģentūrām (CSP) par drošību atbildīgām personām, ja dalībvalsts privātie kodi uzlauzti vai citādi nokļuvuši vai ir aizdomas, ka nokļuvuši, atklātībā.

Šādos gadījumos MSCA vismaz:

- nekavējoties informē MSA, ERCA un visas citas MSCA;

- ir dublēšanas sistēma ar iepriekš ģenerētiem un ERCA sertificētiem MSCA kodu pāriem, kas bez ievērojamas kavēšanās ļauj turpināt MSCA darbību.

6.2.7 Dalībvalsts kodu likvidēšana

MSCA jābūt procedūrai, lai nodrošinātu, ka tai vienmēr ir derīgs, sertificēts dalībvalsts parakstīšanas kodu pāris.

Anulējot dalībvalsts parakstīšanas kodu pāri, publiskais kods jāarhivē un privātais kods:

- jāiznīcina tā, lai privāto kodu nevarētu restaurēt; vai
- jāsaglabā tā, lai to atkārtoti nevarētu izmantot.

6.3 Kustības sensora kodi

Ja nepieciešams MSCA pieprasa ERCA kustības sensoru kodus Km, Km_{VU} un Km_{WC} (Regulas pielikums 1B [REG-A]: papild. 11:3.1.3).

MSCA ievietošanai darbnīcas kartēs nosūta CP tikai darbnīcas kodu Km_{WC}. Darbnīcas kodu Km_{WC} sūta CP šifrētā veidā, izmantojot veidus un līdzekļus, kas minēti ERCA pamatnostādņu pielikumā C [ERCA].

MSCA nepārsūta nedz kustības sensora oriģinālo kodu Km, nedz transportlīdzekļa reģistrācijas ierīces bloka kustības sensora kodu $Km_{WU,}$ kā arī nodrošina, ka tie netiek izmantoti nesankcionētiem mērķiem un ka tie vienmēr atrodas tikai un vienīgi MSCA drošajā vidē..

CP apņemas izpildīt MSCA pienākumu nodrošināt, ka darbnīcas kods Km_{WC} ir ievietots visās izsniegtajās darbnīcas kartē (Regulas pielikums 1B [REG-A]: papild. 11:3.1.3).

MSCA un/vai CP, uzglabājot, izmantojot un ievadot kustības sensora kodu $Km_{WC,}$ nodrošina augstu visa veida drošības līmeni.

Asimetriskos transportēšanas kodus, ko izmanto kustības sensora kodu pieprasīšanai, uzglabāšanai un izsniegšanai, kā arī kustības sensora kodu KM_{wc} ģenerē, uzglabā un lieto speciālā pret viltošanu drošā ierīcē, kas:

- atbilst prasībām, kas noteiktas FIPS 140-2 (vai 140-1) 3. līmenis vai arī augstāks [FIPS]; vai

- ir droša sistēma, kas atbilst EAL 4 vai augstākam standartam saskaņā ar ISO 15408 [CC] vai E3 vai augstākam standartam ITSEC, vai ekvivalentiem drošības kritērijiem. Tam jābūt ar tādu drošības un aizsardzības pakāpi, kas atbilst šo vadlīniju prasībām un izstrādāts balstoties uz riska analīzi un ņemot vērā praktiskos un ar tehniku nesaistītus drošības pasākumus.

6.4 Kodu transportēšana

Visu kodu transportēšanai starp MSCA un ERCA izmanto līdzekļus, starpniekus un protokolus, kas minēti ERCA pamatnostādņu pielikumā C [ERCA]. Ja transportēšanu veic fiziska persona, MSA pilnvaro personu šādu darbību veikt.

MSCA kodu sertificēšanas pieprasīšanai izmanto KCR protokolu, kas aprakstīts ERCA pamatnostādņu pielikumā A [ERCA].

MSCA pieņem tādu ERCA publiskā koda izplatīšanai formātu kā aprakstīts ERCA pamatnostādņu pielikumā B [ERCA].

MSCA nodrošina, ka KID un kodu modulis, kas iesniegts ERCA sertifikācijai un kustības sensora koda izplatīšanai, ir unikāls MSCA domēnā.

MSCA pieprasa ERCA kustības sensora kodu, izmantojot KDR protokolu, kas ietverts ERCA pamatnostādņu pielikumā D [ERCA].

7 Ierīces kodi (asimetriskie)

Ierīces kodi ir asimetriski kodi, ko ģenerē izsniegšanas/ražošanas procesā un sertificē MSCA šādām ierīcēm digitālā tahogrāfa sistēmā:

- tahogrāfa kartes;
- transportlīdzekļa reģistrācijas ierīces bloki (pašlaik un arī tuvākajā nākotnē uz Latviju nav attiecināms).

Simetriskie kustības sensoru kodi šajā dokumentā nav iekļauti.

7.1 Vispārīgie CP/MSCA darbības aspekti, ieskaitot Servisa aģentūras

Ierīces (karšu) inicializēšana, kodu ievietošana un personalizēšana veicama drošā un kontrolētā vietā. Katras personas ieeja šajā zonā stingri regulējama un kontrolējama, bet lietojot sistēmu, jāpiedalās vismaz divām personām. Katra ieiešana drošības zonā un visas darbības sistēmā reģistrējamas.

Slepenā kodu ģenerēšanas sistēmās esošā informācija nedrīkst nonākt ārpus sistēmas tādā veidā, kas ir pretrunā ar šīm vadlīnijām.

Slepenā karšu personalizācijas sistēmā esošā informācija nedrīkst nonākt ārpus sistēmas tādā veidā, kas ir pretrunā ar šīm vadlīnijām.

Organizācijām (apakšlīgumslēdzēji, servisa aģentūras), kas veic kodu ģenerēšanu un karšu personalizāciju vairāk kā vienai dalībvalstij, tas jādara, stingri nošķirot šos procesus katrai valstij atsevišķi. Katrs process jāreģistrē atsevišķi un attiecīgajai MSA pēc pieprasījuma jānodrošina pieeja savas valsts reģistram.

MSCA/CP/ servisa aģentūras: Personalizācijas sistēmas reģistrā jābūt atsaucei uz noteikto kārtību un jābūt attiecīgo ierīču numuru un sertifikātu sarakstam. Attiecīgajai MSA pēc pieprasījuma jānodrošina pieeja savas valsts reģistram.

7.2 Ierīces kodu ģenerēšana

Kodus var ģenerēt vai nu ierīces ražotājs, vai CP, vai MSCA. (Pielikums 1B [REG-A], Papildinājums 11:3.1.1)

Subjektam, kas kodu ģenerē, jānodrošina, ka ierīces kodi tiek ģenerēti drošā vidē un ka ierīces privātā koda glabāšanai nodrošināta slepenība.

Kodu ģenerēšanai jānotiek ierīcē, kas vai nu:

atbilst prasībām, kas noteiktas FIPS 140-2 (vai 140-1) 3. līmenis vai arī augstāks [FIPS]; vai

- atbilst prasībām, kas noteiktas CEN Darbnīcu vienošanās dokumentā 14167-2 [CEN]; vai

- ir droša sistēma, kas atbilst EAL 4 vai augstākam standartam saskaņā ar ISO 15408 [CC] vai E3 vai augstākam standartam ITSEC, vai ekvivalentiem drošības kritērijiem. Tam jābūt ar tādu drošības un aizsardzības pakāpi, kas atbilst šo vadlīniju prasībām un izstrādāts balstoties uz riska analīzi un ņemot vērā praktiskos un ar tehniku nesaistītus drošības pasākumus.

Kodi ģenerējami, izmantojot RSA algoritmu ar moduli koda garumam n=1024 biti (Regulas pielikums1B, papild. 11:2.1/3.2).

Privātā koda ģenerēšanas un uzglabāšanas laikā jānodrošina, lai šis kods nenonāktu ārpus sistēmas, kas to ģenerējusi. Pēc tam, kad šis kods ievietots ierīcē, tas nekavējoties no sistēmas jāizdzēš.

CP atbild par nepieciešamo pasākumu veikšanu, lai nodrošinātu, ka pirms sertifikāta pieprasījuma nosūtīšanas CSP publiskā koda identificētājs ir tam piederošā domēnā vienīgais. (Viens no pasākumiem varētu būt, ka tiek nodrošināts, lai attiecīgās kartes sērijas numurs tiktu izmantots kā koda identificētāja sastāvdaļa un ražošanas procesā tiek saglabāta kartes sērijas numura unikalitāte)

CSP savā domēnā nodrošina publisko kodu unikalitāti tahogrāfu karšu sertifikātos.

Kriptogrāfiskā koda ģenerēšanu var veikt, apstrādājot datus paketē pirms sertifikātu pieprasījuma saņemšanas vai tieši saistībā ar sertifikāta pieprasījumu.

Datu apstrāde paketē veicama ar tīklu nesaistītā ierīcē, ievērojot iepriekš minētos drošības pasākumus. Līdz sertifikāta izsniegšanas brīdim jāsaglabā koda integritāte.

7.3 Ierīces koda derīguma termiņš

7.3.1 Karšu kodi

Ierīces privātā koda, kas izmantots saistībā ar šo vadlīniju ietvaros izsniegtajiem sertifikātiem, derīguma termiņš nedrīkst pārsniegt attiecīgā sertifikāta derīguma termiņu.

7.3.2 Transportlīdzekļa reģistrācijas ierīces bloki

Pašlaik un arī tuvākajā nākotnē uz Latviju nav attiecināms.

7.4 Ierīces privātā koda aizsardzība un glabāšana - kartes

CP garantē, ka karte, kas izsniegta lietotājam kārtībā, kas aprakstīta šajās vadlīnijās, pilnībā nodrošina kartes privātā koda aizsardzību

Privātā koda kopijas glabājamas tikai un vienīgi tahogrāfa kartē, izņemot gadījumus, ja koda ģenerācijas un ierīces personalizācijas procesā noteikta cita kārtība.

Nekādos apstākļos kartes privātais kods nedrīkst nonākt atklātībā vai uzglabāts ārpus kartes.

7.5 Ierīces privātā koda aizsardzība un glabāšana – VU

Pašlaik un arī tuvākajā nākotnē uz Latviju nav attiecināms.

7.6 Ierīces privātā koda reģenerēšana un arhivēšana

Ierīces privātos kodus nevar nedz reģenerēt, nedz arī arhivēt.

7.7 Ierīces publiskā koda arhivēšana

Atbilstoši MSCA, kas veic sertifikāciju, uzdevumam visus sertificētos publiskos kodus arhivē CSP.

7.8 Ierīces kodu likvidēšana

Anulējot tahogrāfa karti, publiskais kods arhivējams, bet privātais kods:

- iznīcināms tā, ka to vairs nav iespējams atjaunot, ja CIA spēj to nodrošināt, vai
- saglabājams tā, lai to vēlreiz vairs nekad nevarētu izmantot.

Izņemot no ekspluatācijas transportlīdzekļa reģistrācijas ierīces bloku, publiskais kods arhivējams, bet privātais kods:

- iznīcināms tā, ka to vairs nav iespējams atjaunot, vai
- saglabājams tā, lai to vēlreiz vairs nekad nevarētu izmantot.

8 Ierīces sertifikāta administrēšana

Šī sadaļa apraksta sertifikāta apriti, ieskaitot reģistrācijas funkciju, sertifikāta izdošanu, izsniegšanu, izmantošanu, atjaunošanu, anulēšanu (ja piemērojama) un likvidēšanu.

8.1 Datu ievadīšana

8.1.1 Tahogrāfa kartes

Karšu īpašniekiem atsevišķi sertifikātu saņemšanai iesniegumi nav jāiesniedz. Sertifikātus izdod, balstoties uz iesniegumā kartes saņemšanai un CIA reģistrā esošo informāciju (sadaļa 5.1.2). Publiskais kods tiek iegūts koda ģenerācijas procesā.

CIA nodrošina, ka ievadāmie dati satur informāciju, kas pilnībā ļauj identificēt sertifikātu īpašnieku. MSCA savā domēnā pārbauda sertifikāta īpašnieks unikalitāti.

Sertifikāta pieprasījuma protokolam jānodrošina, neparādot privāto kodu, pieprasījuma integritāte un izcelsme.

8.3.2 Transportlīdzekļa reģistrācijas ierīces bloki

Pašlaik un arī tuvākajā nākotnē uz Latviju nav attiecināms.

8.2 Tahogrāfa kartes sertifikāti

8.2.1 Vadītāju sertifikāti

Vadītāja sertifikāts tiek izdots tikai tādam iesnieguma iesniedzējam, kura iesniegums apstiprināts un pieņemts lēmums izsniegt vadītāja karti.

8.2.2 Darbnīcu sertifikāti

Darbnīcas sertifikāts tiek izdots tikai tādam iesnieguma iesniedzējam, kura iesniegums apstiprināts un pieņemts lēmums izsniegt darbnīcas karti.

8.2.3 Kontroles sertifikāti

Kontroles sertifikāts tiek izdots tikai tādam iesnieguma iesniedzējam, kura iesniegums apstiprināts un pieņemts lēmums izsniegt kontroles karti.

8.2.4 Uzņēmumu sertifikāti

Uzņēmuma sertifikāts tiek izdots tikai tādam iesnieguma iesniedzējam, kura iesniegums apstiprināts un pieņemts lēmums izsniegt uzņēmuma karti.

8.3 Transportlīdzekļa reģistrācijas ierīces bloku sertifikāti

Pašlaik un arī tuvākajā nākotnē uz Latviju nav attiecināms.

8.4 Ierīces sertifikātu derīguma termiņš

Sertifikātu derīguma termiņš nevar pārsniegt attiecīgās ierīces derīguma termiņu.

- Vadītāju sertifikātu derīguma termiņš nevar pārsniegt **5** gadus.
- Darbnīcas sertifikātu derīguma termiņš nevar pārsniegt **1** gadu.
- Kontroles sertifikātu derīguma termiņš nevar pārsniegt **2** gadus.
- Uzņēmuma sertifikātu derīguma termiņš nevar pārsniegt **5** gadus.

8.5 Ierīces sertifikātu izdošana

MSCA nodrošina, ka, izdodot sertifikātus, tiek saglabāta to autentiskums un integritāte. Sertifikātu saturs noteikts Regulas pielikumā 1B [REG-A], papildinājums 11.

8.6 Ierīces sertifikātu atjaunošana

Skatīt 5. sadaļu „Ierīces administrēšana” Tā kā sertifikātiem un kartēm ir vienāds derīguma termiņš, tad tie apskatāmi kopā. VU sertifikāti ir vai nu beztermiņa, vai arī tiem ir ļoti ilgs derīguma termiņš. Tiek uzskatīts, ka ierīces kalpošanas laiks ir īsāks par sertifikāta kalpošanas laiku.

8.7 Ierīces sertifikātu un informācijas izplatīšana

CIA nodrošina, ka nepieciešamības gadījumā sertifikāti pieejami attiecīgi lietotājiem un iesaistītajām pusēm.

CIA nodrošina, ka visi izdošanas nosacījumi, ar to saistītās CSP PS sadaļas un cita nepieciešamā informācija pieejama visiem lietotājiem, iesaistītajām pusēm un citām ar to saistītām personām.

8.8 Ierīces sertifikātu lietošana

Digitālo tahogrāfu sertifikāti lietojami tikai digitālo tahogrāfu sistēmā.

8.9 Ierīces sertifikātu anulēšana

Sertifikāti nav atsaucami, bet MSCA jānodrošina sertifikātu statusa uzskaite un šīs informācijas pieejamība pēc to pieprasījuma tādām iesaistītām pusēm kā:

- MSA un dalībvalstu kontroles institūcijas;
- ES Komisija

9 MSCA, CIA, CP, CSP informācijas drošības administrēšana

Katrai iesaistītajai pusei jāveido sava informācijas drošības dokumentācijas uzskaite. Puses paraksta vienošanos par informācijas drošību, kurā ietverts detalizēts vispārējo drošības procedūru apraksts katrai pusei.

Katra puse apstiprina savu informācijas drošības administrēšanas sistēmu, kas atbilst BS7799 [ISO 17799] standartam. Oficiāls sertifikāts nav vajadzīgs.

Katra puse nodrošina, ka tās rīcībā visu laiku būs personāls, kas vismaz:

- ir apmācīts veikt uzticētos uzdevumus digitālā tahogrāfa sistēmā;
- zina savus darba uzdevumus digitālā tahogrāfa sistēmā;
- nav bijis iesaistīts noziedzīgās darbībās un to ir apliecinājusi policija vai līdzīga institūcija.

Katra puse nodrošina, ka tiek saglabāts tās darbību reģistrs un ka tai ir instrukcija, kas nosaka šādu reģistru glabāšanas ilgumu.

10 MSCA vai CP darbības pārtraukšana

10.1 Pilnīga darbības pārtraukšana - MSA atbildība

Par MSCA vai CIA pilnīgu darbības pārtraukšanu uzskatāma situācija, kad visi ar MSCA vai CIA saistītie pakalpojumi tiek pilnībā pārtraukti. Par tādu situāciju nav uzskatāms gadījums, kad viena organizācija attiecīgā pakalpojuma sniegšanu nodod citai vai kad MSCA pakalpojums ar veco dalībvalsts kodu pāri tiek aizstāts ar jaunu dalībvalsts kodu pāri vai ERCA kodu. Tā ietver arī situāciju, kad dalībvalsts no digitālā tahogrāfa sistēmas izstājas vai arī visa šī sistēma beidz pastāvēt.

MSA nodrošina, ka tiek veikti turpmāk minētie uzdevumi.

Pirms MSCA/CIA beidz savu darbību tai vismaz jāveic šādi uzdevumi:

a) jāinformē visi lietotāji un puses, ar ko MSCA/CIA noslēgusi līgumus vai tai ir cita veida saistības;

b) vismaz **3** mēnešus pirms savas darbības izbeigšanas par to jāpaziņo publiski;

c) MSCA/CIA jāpārtrauc visu apakšlīgumslēdzējiem izsniegto pilnvarojumu darbība sertifikātu izdošanas procesā rīkoties MSCA/CIA vārdā;

d) MSCA/CIA jāveic nepieciešamie pasākumi, lai saglabātu un nodrošinātu pieejamību darbības reģistra arhīviem.

10.2 CSP vai CP pienākumu nodošana

CSP vai CP pienākumu nodošana notiek, kad MSA ir izvēlējusies jaunu CSP vai CP iepriekšējo vietā.

MSA nodrošina, ka pienākumu un īpašuma nodošana notiek noteiktajā kārtībā.

Iepriekšējā CSP nodod visus publiskos kodus jaunajai CSP kārtībā, kādu noteikusi MSA.

Iepriekšējā CSP iznīcina visas MSCA kodu kopijas.

11 Audits

MSA ir atbildīga, ka tiek organizēts audits CP un CSP. Audita ziņojumiem jābūt pieejamiem angliski.

11.1 Iesaistīto subjektu audita biežums

Lai pārbaudītu atbilstību nacionālajām MSA vadlīnijām, CP un CSP, kas veic darbības šo vadlīniju ietvaros, auditējams vismaz vienu reizi divos gados.

11.2 Auditā iekļaujamie aspekti

Auditā iekļaujams MSCA/CP/CSP darbības apraksts.

Auditā iekļaujams MSCA/CP/CSP atbilstība nacionālajām MSA vadlīnijām.

Auditā jāiekļauj arī visu servisa aģentūru darbība.

Par audita rezultātiem sagatavojams audita ziņojums, kurā ietver koriģējošo pasākumu plānu kopā ar izpildes grafiku, kurā jāpanāk atbilstība vadlīniju prasībām.

Auditā iekļaujams CP un CSP atbilstība prasībām, kas minētas ERCA – CP § 5.3

11.3 Kas veic auditu

Lai apstiprinātu CP/CSP/ PS un palielinātu iesaistīto pušu uzticamību sistēmas pareizai ieviešanai, MSA var konsultēties ar ārvalstu sertifikācijas vai akreditācijas iestādēm. Ja nav iespējams saņemt palīdzību, MSA jāveic auditēšana pašai.

11.4 Pasākumi, kas veicami, konstatējot nepilnības

Ja audita laikā darbībā tiek konstatēti trūkumi, MSA piemēro sankcijas, ņemot vērā pārkāpumu nopietnību.

11.5 Audita rezultātu pieejamība

Audita rezultāti par drošības līmeni pieejami tikai pēc pieprasījuma. Audita ziņojumiem pilnībā nav jābūt pieejamiem, izņemot gadījumos, kad to nosaka īpaša kārtība Audita ziņojumi iesniedzami ERCA.

12 Nacionālo MSA vadlīniju grozīšanas kārtība

12.1 Aspekti, ko iespējams mainīt bez notifikācijas

Vienīgās izmaiņas, ko iespējams veikt bez paziņošanas ir:

a) redakcionāla rakstura vai teksta izkārtojuma labojumi;

b) izmaiņas kontaktinformācijā.

12.2 Grozījumi, piemērojot notifikāciju

12.2.1 Paziņojums

Jebkuru punktu šajās vadlīnijās iespējams grozīt, par to vismaz **90** dienas paziņojot iepriekš.

Izmaiņas punktos, kas pēc par vadlīnijām atbildīgās institūcijas domām (MSA) būtiski **neietekmē** lielāko daļu lietotāju vai ar šīm vadlīnijām saistītās puses, var izdarīt, par to vismaz **30** dienas paziņojot iepriekš.

12.2.2 Komentāru sniegšanas periods

Lietotāji, kurus grozījumi ietekmē, var 15 dienu laikā kopš paziņojuma par grozījumu izdarīšanas dienas par vadlīnijām atbildīgai institūcijai sniegt savus komentārus.

12.2.3 Ko informēt?

Informācija par izmaiņām šajās vadlīnijās nosūtāma:

- ERCA
- MSCA un CIA, ieskaitot servisa aģentūras
- visas citas MSAs

12.2.4 Periods grozījumu galīgās redakcijas paziņošanai

Ja ierosinātie grozījumi, ņemot vērā sniegtos komentārus, tiek mainīti, paziņojums par izdarītajām izmaiņām grozījumā sniedzams vismaz **30** dienas pirms šo grozījumu stāšanās spēkā.

12.3 Izmaiņas, kuru dēļ nacionālās MSA vadlīnijas nepieciešams apstiprināt vēlreiz

Ja MSA noteiktās izmaiņas vadlīnijās būtiski ietekmē ievērojamu šo vadlīniju lietotāju, MSA iesniedz grozītās nacionālās MSA vadlīnijas ERCA apstiprināšanai.

13 Atsauces

[REG] Padomes Regula (EEK) Nr.3821/85, ko groza ar Padomes 1998. gada 24. septembra Regulu (EK) Nr. 2135/98

[REG-A] Padomes Regulas(EK) Nr. 2135/98 Pielikums I(B) *Prasības uzbūvei, testēšanai, uzstādīšanai un kontrolei*

[BPM] Digitālā tahogrāfa karšu izdošanas rokasgrāmata. Karšu izdošanas darba grupa, 2003.gada 15. decembris, Komisijas īpašums

[CC] Vienotie kritēriji. ISO/IEC 15408 (1999): "Informācijas tehnoloģijas – Drošības tehnoloģija – IT drošības novērtēšanas kritēriji (1. – 3. daļa)".

[CEN] CEN Darbnīcu vienošanās 14167-2: Kriptogrāfiskais modulis CSP parakstīšanas operācijām – Aizsargprofils (MCSO-PP)

[ETSI 102 042] ETSI TS 102 042. Pamatprasības sertifikācijas institūcijām, kas izsniedz publiskā koda sertifikātus

[FIPS] FIPS PUB 140-2 (2001.gada 25.maijs): "Drošības prasības kriptogrāfiskiem moduļiem ". Informācijas tehnoloģiju laboratorija, Nacionālais standartu un tehnoloģiju institūts (NIST)

[ISO 17799] BS ISO/IEC 17799: 2000. Informācijas tehnoloģijas – Standarts informācijas drošības vadībai.

[CSG] Vispārīgās drošības vadlīnijas, Karšu izdošanas projekts, Komisijas īpašums

[ERCA] Eiropas galvenās digitālā tahogrāfa sistēmas pamatnostādnes, versija 2.0, speciālizdevums I.04.131

14 Glosārijs/definīcijas un saīsinājumi

14.1 Glosārijs/definīcijas

MSA vadlīnijas: noteikumu kopums, kas nosaka, kā izmantot kodus, sertifikātus un ierīci īpašai personu un ierīču kategorijai, ievērojot vienotas drošības prasības.

Karte/tahogrāfa karte: karte ar integrēta mikroshēmu, kas šajās vadlīnijās ir ekvivalents terminiem ”IC karte” un ”viedkarte”.

Kartes īpašnieks: fiziska vai juridiska persona, kurai pieder un kas lieto tahogrāfa karti. Šajā skaitā ietilpst autovadītāji, uzņēmumu pārstāvji, darbnīcu darbinieki un kontrolieri.

Sertifikāts: Pamatā sertifikāts ir ziņojuma struktūra, kas ietver izdevēja parakstu, kurš apliecina, ka sertifikātā ievadītā informācija ir pareiza un ka sertificētā publiskā koda īpašnieks var pierādīt, ka tam ir attiecīgs privātais kods.

Sertifikācijas institucionālā sistēma (CAS): datorsistēma, kurā sertifikāti tiek izdoti, apliecinot sertifikāta (lietotāja) datu pareizību ar CA privāto parakstīšanās kodu.

Sertifikācijas darbības apraksts (CPS): darbību uzskatījums, kuru izpilde sertifikācijas institūcijai, izdodot sertifikātus, jānodrošina un kas atbilst šīm MSA vadlīnijām.

Ierīce: Digitālā tahogrāfa sistēmā ir šādas ierīces: tahogrāfa kartes, VU (transportlīdzekļa reģistrācijas ierīču bloki) un kustības sensori.

Ražotājs/Ierīces ražotājs: Tahogrāfa ierīču ražotāji. Šajās vadlīnijās visbiežāk lietots termins saistībā ar VU un kustības sensoru ražotājiem, jo tiem ir svarīga loma digitālā tahogrāfa sistēmā.

Kustības sensoru kods: simetrisks kods, ko izmanto kustības sensoros un VU, lai nodrošinātu savstarpēju atpazīstamību.

Darbības apraksts: Drošības pasākumu apraksts, kas jāievēro digitālā tahogrāfa sistēmā. PS pielīdzināms standarta PKI dokumentam CPS.

Privātais kods: asimetriskā kodu pāra privātā daļa, ko izmanto publiskā koda kriptēšanas procesā. Parasti privāto kodu izmanto, lai parakstītos digitāli vai atšifrētu ziņojumus. To sauc arī par slepeno kodu.

Publiskais kods: asimetriskā kodu pāra publiskā daļa, ko izmanto publiskā koda kriptēšanas procesā. Parasti publisko kodu izmanto, lai salīdzinātu digitālos parakstus vai atšifrētu privāta koda īpašnieka ziņojumus.

RSA kodi: RSA ir kriptogrāfisks algoritms, ko izmanto asimetrisku (PKI) kodu ģenerēšanai digitālā tahogrāfa sistēmā.

Servisa aģentūra: Uzņēmums, kas kā apakšlīgumslēdzējs apņemas veikt uzdevumus, ko tam uzticējusi MSCA, CIA vai CP.

Tahogrāfa kartes /Kartes: Četru veidu viedkartes izmantošanai digitālā tahogrāfa sistēmā: Vadītāja karte, Uzņēmuma karte, Darbnīcas karte, Kontroles karte.

Lietotājs: Lietotāji ir iekārtas izmantotāji. Tie ir vai nu karšu īpašnieki attiecībā uz kartēm, vai arī ražotāji attiecībā uz transportlīdzekļu reģistrācijas ierīču blokiem/kustības sensoriem. Visiem lietotājiem jābūt konkrēti identificējamiem subjektiem.

Šajā dokumentā:

Paraksts: Gadījumos, kad vadlīnijās norādīts, ka nepieciešams paraksts, prasība izpildīta, ja izmantots drošs un pārbaudāms digitālais paraksts.

Rakstiski: Gadījumos, kad vadlīnijās norādīts, ka nepieciešams sniegt informāciju rakstiski, prasība izpildīta, ja iesniegta datne, un tajā ietverto informāciju puses, kurām tā nepieciešama, var bez sarežģījumiem izmantot.

14.2 Saīsinājumi

CA	Sertifikācijas institūcija
CAS	Sertifikācijas institucionālā sistēma
CIA	Karšu izsniegšanas institūcija
CC	Vienotie kritēriji
CP	Karšu personalizācijas veicējs
CP PS	Karšu personalizācijas veicēja darbības apraksts
CPS	Sertifikācijas veicēja darbības apraksts
CSP	Sertifikācijas veicējs
DB	Datu bāze
ERCA	Eiropas Galvenā sertifikācijas institūcija
HSM	Aparatūras drošības modulis
ISSO	Atbildīgais par informācijas sistēmas drošību
ITSEC	Informācijas tehnoloģijas drošības vērtēšanas kritēriji
KG	Kodu ģenerēšana
MS	Digitālo tahogrāfu sistēmas dalībvalsts
MSA	Dalībvalsts kompetentā institūcija
MSCA	Dalībvalsts sertifikācijas institūcija
PIN	Personīgais identifikācijas numurs
PKI	Publiskā koda infrastruktūra
RSA	Īpašs publiskā koda algoritms
SA	Sistēmas administrators
PS	Darbības apraksts
VU	Transportlīdzekļa reģistrācijas ierīces bloks
VUP	VU personalizācijas veicējs

15. Atbilstības ERCA pamatnostādnēm izvērtējuma tabula

Šī tabula parāda Latvijas kompetentās institūcijas digitālā tahogrāfa sistēmai nacionālo vadlīniju atbilstību ERCA pamatnostādņu [ERCA] 5.3 nodaļas prasībām.

ERCA CP	LV MSA	Piezīmes
§5.3.1	§1.1	CPS iesaistītajiem subjektiem. Par to tiks informēta ERCA.
§5.3.2	§6.2.1, §6.2.3, §6.3	CPS tiks noteikts kādu (sertificētu) HSM ierīci izmantos. CPS būs pieejams ERCA
§5.3.3	§6, §6.2.1	CPS tiks noteikts, kādas drošības kontroles sistēmas tiks izmantotas. Par to tiks informēta ERCA
§5.3.4	§6.2.2	
§5.3.5	§6.2.1	
§5.3.6	§6.4	
§5.3.7	§6.4	
§5.3.8	§6.4	
§5.3.9	§6.4	
§5.3.10	§6.4	
§5.3.11	§6.2.7	
§5.3.12	§7.1, §7.2, §5.1.1	CP PS tiks noteikts kādu (sertificētu) HSM ierīci izmantos. Par to tiks informēta ERCA. CP PS tiks noteikts kādu (sertificētu) karti izmantos. Par to tiks informēta ERCA.
§5.3.13	§3.4.1, §6.2.1, §7.2	
§5.3.14	§6.2.3, §7.3, §7.4	
§5.3.15	§6.2.4	
§5.3.16	§7.2	
§5.3.17	§6.2.5, § 7.6	
§5.3.18	§6.3	
§5.3.19	§6.3	
§5.3.20	§6.3	Nav attiecināms.
§5.3.21	§6.3	
§5.3.22	§3.1.9, §6.3	Nav attiecināms.
§5.3.23	§3.4.1, §6.3	

ERCA CP	LV MSA	Piezīmes
§5.3.24	§6.3	
§5.3.25	§6.2, §6.3, §7.5	Latvijas MSA vadlīnijās VU-ražotāji nav iekļauti
§5.3.26	§6.2.1	
§5.3.27	§6.2	
§5.3.28	§6.2.3	
§5.3.29	§7.2	
§5.3.30	§7.3 §8.1.1	
§5.3.31	§5.1.6 §8.9	
§5.3.32	§8.4	
§5.3.33, §5.3.34		Nav attiecināms, jo Latvijas MSA vadlīnijās beztermiņa sertifikāti nav iekļauti (nepieciešami VU-ražotājiem)
§5.3.35	§5.1.2, §5.1.10	
§5.3.36	§6.2.6	
§5.3.37	§6.2.6	
§5.3.38	§9	
§5.3.39	§9	
§5.3.40	§9	
§5.3.41	§10	
§5.3.42	§12	
§5.3.43	§11.2	
§5.3.44	§11.1	
§5.3.45	§11, §11.5	
§5.3.46	§11,2, §11.4	