

## Tirgotāju atbilstība SEPA Maksājumu karšu nozares standartiem

### Maksājumu karšu nozares standarti

- Maksājumu karšu nozares Datu drošības standarts – minimālās drošības prasības, kuras jāievēro katram, kas apstrādā, glabā un pārraida karšu darījumus.
- Maksājumu karšu nozares PIN drošības standarts – minimālās drošības prasības, kuras jāievēro katram, kas apstrādā un pārraida PIN kodus.
- Maksājumu aplikāciju Datu drošības standarts – minimālās drošības prasības programmatūrai, kas apstrādā karšu darījumus.

### Ieteikumi viedkaršu pieņemšanas un PIN ievades iekārtu iegādei

- Viedkaršu pieņemšanas iekārtām to iegādes brīdī jābūt derīgiem šādiem EMVCo sertifikātiem:
  - *EMVCo Type 1 Approval*;
  - *EMVCo Type 2 Approval*.
- Stingri iesakām pirms iegādes pārliecināties par izvēlētas iekārtas atbilstību, pieprasot attiecīgo informāciju no piegādātāja un pārbaudot to interneta resursā [www.emvco.com](http://www.emvco.com).
- Iekārtām, kuras tiks izmantotas PIN koda ievadei, obligāti jābūt sertificētām.
- Stingri iesakām uzņēmumam pirms šo iekārtu iegādes pieprasīt iekārtu piegādātājam informāciju par PIN ievades iekārtas modeli, sērijas numuru (*hardware number*) un programmatūras versiju (*firmware number*).
- Modelim un sērijas numuram, un programmatūras versijai jāsakrīt ar interneta resursā [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org) publicēto informāciju. Ja kaut viens no minētajiem komponentiem nesakrīt, PIN ievades iekārtu nedrīkst ekspluatēt.
- Iesakām pirms PIN ievades iekārtu iegādes pārbaudīt tās lietošanas derīguma termiņu.

PIN standarta versija, saskaņā ar kuru iekārta sertificēta	Sertifikācijas derīguma termiņš	Ekspluatācijas beigu termiņš**
1.x	2014. gada 30. aprīlis*	Pašlaik nav noteikts
2.x	2017. gada 30. aprīlis*	Pašlaik nav noteikts
3.x	2020. gada 30. aprīlis*	Pašlaik nav noteikts
Pre-PCI***	2007. gada 31. decembris*	2012. gada 31. decembris****
Visas citas iekārtas	-	2010. gada 30. jūnijs****

\*[https://www.pcisecuritystandards.org/security\\_standards/ped/pedapprovallist\\_footnotes.html#4](https://www.pcisecuritystandards.org/security_standards/ped/pedapprovallist_footnotes.html#4).

\*\*PCI standartam atbilstošo iekārtu ekspluatācijas beigu termiņu nosaka starptautiskās maksājumu karšu organizācijas.

\*\*\*Iekārtas, kuras neatbilst PCI standartam, bet kuru izmantošanu apstiprinājušas starptautiskās maksājumu karšu organizācijas.

\*\*\*\*[http://www.sepalatvija.lv/sites/default/files/20100506\\_Par\\_VISA\\_MC\\_parmainaam.pdf](http://www.sepalatvija.lv/sites/default/files/20100506_Par_VISA_MC_parmainaam.pdf).

- Ja uzņēmumā plānots izmantot PIN kodu kartes lietotāja pārbaudei visiem karšu darījumiem (arī kartēm ar magnētisko celiņu), papildus jāievēro šādi nosacījumi:
  - nešifrēts PIN kods drīkst atrasties tikai drošā fiziskā iekārtā (*Tamper Resistant Security Module*; TRSM);
  - PIN transakciju šifrēšanas iekārtām (*Hardware Security Module*; HSM) jāatbilst *FIPS 140.2 Level 3* standartam;

- PIN kods ārpus drošās iekārtas obligāti jāšifrē, izmantojot *TripleDES* šifrēšanas algoritmu.
- Videonovērošanas iekārtām jābūt orientētām tā, lai ierakstā nebūtu redzama ne PIN koda ievades tastatūra, ne arī tas, kā kartes lietotājs ievada PIN kodu.

Starptautiskās karšu organizācijas izdod noteikumus par karšu drošības prasībām, kas nosaka specifiskas prasības karšu pieņēmējiem – tirgotājiem un maksājumu apstrādes centriem.

Līmenis	Tirgotājs	Prasība
1. līmenis	Tirgotāji, kuru karšu darījumu skaits gadā pārsniedz 6 milj. vai pie kuriem notikusi karšu datu zādzība.	Reizi gadā <u>sertificēts auditors</u> veic auditu vai <u>sertificēts iekšējais auditors</u> aizpilda pašnovērtējuma anketu. Reizi ceturksnī veic uzņēmuma datortīkla ārējo pārbaudi.
2. līmenis	Tirgotāji, kuru karšu darījumu skaits gadā ir 1–6 milj.	Reizi gadā <u>sertificēts iekšējais auditors</u> aizpilda pašnovērtējuma anketu vai <u>sertificēts auditors</u> veic auditu. Reizi ceturksnī veic uzņēmuma datortīkla ārējo pārbaudi.
3. līmenis	E-komercijas tirgotāji, kuru darījumu skaits gadā ir 20 tūkst.–1 milj.	Reizi gadā aizpilda pašnovērtējuma anketu ( <i>self-assessment questionnaire</i> ). Reizi ceturksnī veic uzņēmuma datortīkla ārējo pārbaudi.
4. līmenis	Visi citi tirgotāji, kuru karšu darījumu skaits gadā ir līdz 1 milj.	Pieņēmējbanka nosaka veicamās darbības.

Maksājumu karšu nozares Datu drošības standarts: **pašnovērtējums**

- Aktuālā versija pieejama PCI interneta resursā ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)).
- Pašnovērtējuma apjoms atkarīgs no tirgotāja specifikas:
  - e-komercijas tirgotāji, kuri izmanto *First Data* piegādāto IBIS risinājumu un paši neapstrādā karšu datus, aizpilda "A" variantu;
  - tirgotāji, kuri kartes pieņem ar imprinteri un/vai atsevišķu POS termināli un karšu datus neglabā elektroniski, aizpilda "B" variantu;
  - tirgotāji, kuri kartes pieņem POS sistēmās/kasu sistēmās, kuras karšu datus sūta pa internetu, bet tos neglabā elektroniski, aizpilda "C" variantu;
  - tirgotāji, kuri neietilpst nevienā no minētajām kategorijām, aizpilda "D" variantu.