DROŠA LIETOTĀJU AUTENTIFICĒŠANA, SNIEDZOT MAKSĀJUMU PAKALPOJUMU

STRONG CUSTOMER AUTHENTIFICATION WHEN PROVIDING A PAYMENT SERVICE

Anete Bože
Rīgas Stradiņa universitāte, Mg. iur. anete.boze@mail.com, Rīga, Latvija

Abstract. *Strong customer authentication in the Second Payment Service Directive means customer authentication where customer shall use two or more of the following elements: knowledge (what only the user knows), possession (what only is in the user's possession) and inherence (user-specific).*

The purpose of the strong customer authentication is to make payment services more secure and to protect costumer's personal data. It is mandatory to use at least two of three elements: elements: knowledge, such as password, numeric code, pet name, etc., possession, such as a mobile phone, and inherence, such as a fingerprint.

The aim of the article is to find out what is secure customer authentication, what it contains and in which cases secure user authentication does not apply.

Keywords: *Payment Services, PSD2, Strong Customer Authentication.*

Ievads

2016. gada 12. janvārī stājās spēkā Eiropas Parlamenta un Padomes direktīva (ES) 2015/2366 (2015. gada 25. novembris) par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 2002/65/EK, 2009/110/EK un 2013/36/ES un Regulu (ES) Nr. 1093/2010 un atceļ Direktīvu 2007/64/EK, kas ir pazīstama arī kā Otrā maksājumu pakalpojumu direktīva.

Otrā maksājumu pakalpojumu direktīva pieprasa, ka noteiktos gadījumos, sniedzot maksājumu pakalpojumus, maksājumu pakalpojumu sniedzējam ir jāpiemēro droša klientu autentifikācija, kas paredz, ka klienta autentificēšanai tiek izmantotas vismaz divi no trim elementiem sekojošiem elementiem: zināšanas (to, ko zina tikai lietotājs), valdījums (to, kas ir tikai lietotāja valdījumā) un neatņemamas īpašības (lietotājam raksturīgas īpašības), *(Par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 2002/65/EK, 2009/110/EK un 2013/36/ES un Regulu (ES) Nr. 1093/2010 un atceļ Direktīvu 2007/64/EK, 2015, 97.p. 1.daļa).*

Atbilstoši Otrajai maksājumu pakalpojumu direktīvai Eiropas Banku iestādei (*European Banking Authority*) ir pienākums izstrādāt regulatīvos tehniskos standartus (*Par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 2002/65/EK, 2009/110/EK un 2013/36/ES un Regulu (ES) Nr. 1093/2010 un atceļ Direktīvu 2007/64/EK, 2015, 98. p. 1.daļa)*, kas cita starpā nodrošinātu atbilstošu drošo klientu autentificēšanu. 2018. gada 14.martā stājās spēkā Komisijas deleģētā regula (ES) 2018/389 (2017. gada 27. novembris), ar ko Eiropas Parlamenta un Padomes Direktīvu (ES) 2015/2366 papildina attiecībā uz regulatīvajiem tehniskajiem standartiem par drošu lietotāja autentificēšanu un vienotiem un drošiem atklātiem saziņas standartiem (turpmāk – Regula 2018/389), kuras viens no priekšmetiem ir piemērot drošas lietotāju autentificēšanas procedūru *(Ar ko Eiropas Parlamenta un Padomes Direktīvu (ES) 2015/2366 papildina attiecībā uz regulatīvajiem tehniskajiem standartiem par drošu lietotāja autentificēšanu un vienotiem un drošiem atklātiem saziņas standartiem, 2017, 1.p.).*

Līdz ar to droša lietotāju autentificēšana ir samērā jauns priekšnosacījums maksājumu pakalpojumu nodrošināšanai, kas prasa padziļinātu izpēti.

Šī raksta mērķis ir noskaidrot normatīvo aktu prasības attiecībā uz drošu lietotāju autentificēšanu, konstatēt, kādi ir droši lietotāju autentificēšanas elementi, ko tie ietver, kā arī priekšnosacījumus, kad

https://doi.org/10.17770/iss2021.6909

drošā lietotāju autentificēšana var netikt piemērota un iespējamos riskus.

Rakstā tika izmantotas vispārzinātniskās pētījumu metodes un tiesību normu interpretācijas metodes. Vienlaikus tika analizēti Eiropas Savienības normatīvie akti, kā arī veikta dokumentu analīze.

Nepieciešamība pieņemt Otro maksājumu pakalpojumu direktīvu

Līdz Otrās maksājumu pakalpojumu direktīvas spēkā stāšanās spēkā bija, tā saucamā, Pirmā maksājumu pakalpojumu direktīva jeb Eiropas Parlamenta un Padomes direktīva 2007/64/EK (2007. gada 13. novembris) par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 97/7/EK, 2002/65/EK, 2005/60/EK un 2006/48/EK un atceļ Direktīvu 97/5/EK.

2013. gada 24. jūlijā Eiropas Komisija izstrādāja priekšlikumu Pirmās maksājumu pakalpojumu direktīvas atcelšanai, kurā norāda uz šādiem aspektiem, kādēļ ir nepieciešama jauna maksājumu pakalpojumu direktīva: "Šī iniciatīva ļaus patērētājiem un tirgotājiem pilnībā izmantot iekšējā tirgus priekšrocības, īpaši e-komercijas jomā. Šā priekšlikuma mērķis ir palīdzēt turpmāk attīstīt Eiropas Savienības mēroga elektronisko maksājumu tirgu, kas ļaus patērētājiem, mazumtirgotājiem un citiem tirgus dalībniekiem pilnībā izmantot ES iekšējā tirgus sniegtās priekšrocības atbilstīgi stratēģijai "Eiropa 2020" un Eiropas digitalizācijas programmai. Šāda ciešāka integrācija kļūst aizvien svarīgāka, jo pasaulē notiek pāreja no vienkāršas tirdzniecības uz digitālu ekonomiku. Lai to panāktu un lai veicinātu lielāku konkurenci, efektivitāti un inovācijas e-maksājumu jomā, būtu jābūt juridiskai skaidrībai un vienādiem noteikumiem, kā rezultātā samazinātos izdevumi un cenas maksājumu pakalpojumu lietotājiem, tiktu nodrošināta lielāka maksājumu pakalpojumu izvēle un pārredzamība, atvieglota novatorisku maksājumu pakalpojumu sniegšana un nodrošināti droši un pārredzami maksājumu pakalpojumi" *(Eiropas Komisija, 2013)*.

Būtiski ir norādīt, kam ir arī nozīme attiecībā uz drošu lietotāju autentificēšanu, ka ar Otro maksājumu pakalpojumu direktīvu tika ieviesta arī "tehnoloģiskā neitralitāte" attiecībā uz maksājumu pakalpojumiem. Proti, "tehnoloģiskā neitralitāte" paredz, ka maksājumu pakalpojumu definīcijai vajadzētu būt tehnoloģiski neitrālai un būtu jāļauj attīstīties jauniem maksājumu pakalpojumu veidiem, vienlaikus nodrošinot līdzvērtīgus darbības apstākļus gan esošajiem, gan jaunajiem maksājumu pakalpojumu sniedzējiem (sk. Otrās maksājumu pakalpojumu direktīvas 21. ievadapsvērumu). Tādējādi maksājumu pakalpojumu sniegšanā var tikt izmantoti visdažādākie tehnoloģiskie risinājumi. Vēl jo vairāk – Otrā maksājumu pakalpojumu direktīva veicina jaunu tehnoloģisku risinājumu izmantošanu maksājumu pakalpojumu sniegšanā. Uzskatāms, ka Otrā maksājumu pakalpojumu direktīva ir zināmā mērā sasniegusi minēto mērķi, jo maksājumu pakalpojumu sniegšanā tiek izmantoti arī ļoti inovatīvi tehnoloģiskie risinājumi, piemēram, mākslīgais intelekts *(Eiropas Komisija, 2013)*.

Secināms, ka Otrās maksājumu pakalpojumu direktīvas mērķis ir cieši saistīts ar straujo tehnoloģisko attīstību, digitalizāciju, konkurences veicināšanu un efektivitāti. Droša lietotāju autentificēšana, viennozīmīgi, ir cieši saistīta ar jaunu tehnoloģisko risinājumu rašanos. Visticamāk, ka laikos, kad viedtālrunis nebija pieejams teju ikkatram, droša lietotāju identificēšana nevarētu tikt realizēta, jo viens no drošas lietotāju autentificēšanas elementiem ir autentificēt lietotāju, izmantojot kaut ko, kas ir lietotāja īpašumā, piemēram, viedtālrunis. Tādējādi, ņemot vērā tehnoloģiskās iespējas, Otrā maksājumu pakalpojumu direktīva pieprasīja maksājumu pakalpojumu sniedzējiem veikt šo drošo lietotāju autentificēšanu.

Drošas lietotāju autentificēšanas elementi

Saskaņā ar Otrās maksājumu pakalpojumu direktīvas 4. panta 30. punktu "droša lietotāju autentificēšana" ir autentificēšana, izmantojot divus vai vairākus elementus, ko klasificē kā zināšanas (to, ko zina tikai lietotājs), valdījumu (to, kas ir tikai lietotāja valdījumā) un neatņemamas īpašības (lietotājam raksturīgas īpašības) un kas ir savstarpēji neatkarīgi, proti, neatbilstība vienam kritērijam neapdraud pārējo elementu uzticamību, un kas ir izstrādāti tā, lai nodrošinātu autentificēšanas datu konfidencialitātes aizsardzību *(Par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 2002/65/EK, 2009/110/EK un 2013/36/ES un Regulu (ES) Nr. 1093/2010 un atceļ Direktīvu 2007/64/EK, 2015, 4.p. 30.punkts)*.

No minētā secināms, ka droša lietotāju autentificēšanai jāizmanto vismaz divi no trim elementiem:

1) zināšanas (to, ko zina tikai lietotājs);
2) valdījumu (to, kas ir tikai lietotāja valdījumā);
3) neatņemamas īpašības (lietotājam raksturīgas īpašības) (Eiropas Parlamenta un Padomes direktīva (ES) 2015/2366 *(Par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 2002/65/EK, 2009/110/EK un 2013/36/ES un Regulu (ES) Nr. 1093/2010 un atceļ Direktīvu 2007/64/EK, 2015, 4.p. 30.punkts)*.

Otrā maksājumu pakalpojumu direktīva plašāk nepaskaidro iepriekš minēto elementu saturu, bet plašāku skaidrojumu sniedz Regula 2018/389. Proti, Regulas 2018/389 ievadapsvērumu 6. punkts nosaka: "Lai nodrošinātu, ka tiek piemērota droša klienta autentificēšana, ir svarīgi arī pieprasīt, lai būtu atbilstoši drošības parametri attiecībā uz drošas klienta autentificēšanas elementiem, ko kategorizē kā zināšanas (kaut kas, ko zina tikai lietotājs), piemēram, elementa garums vai sarežģītība, kā valdījumu (kaut kas, kas ir tikai lietotāja valdījumā), piemēram, algoritmu specifikācijas, atslēgas garums un entropija, un attiecībā uz ierīcēm un programmatūru, kas nolasa elementus, kuri klasificēti kā neatņemamas īpašības (kaut kas, kas lietotājs ir), piemēram, algoritmu specifikācijas, biometriskie sensori un veidnes aizsardzības elementi, jo īpaši lai mazinātu risku, ka nepiederošas personas šos elementus atklāj, izpauž un izmanto. [..]." *(Ar ko Eiropas Parlamenta un Padomes Direktīvu (ES) 2015/2366 papildina attiecībā uz regulatīvajiem tehniskajiem standartiem par drošu lietotāja autentificēšanu un vienotiem un drošiem atklātiem saziņas standartiem, 2017, ievadapsvērumu 6.punkts)*.

Eiropas Banku iestāde, izstrādājot regulatīvi tehniskos standartus (Direktīvu 2015/2366), ir publicējusi arī konsultāciju ziņojumu, kurā norāda, ka: "Eiropas Banku iestāde piekrīt dalībnieku viedoklim, ka, lai nodrošinātu tehnoloģiju un uzņēmējdarbības modeļa neitralitāti un ļautu maksājumu pakalpojumu sniedzējiem nepārtraukti pielāgoties mainīgajiem krāpšanās scenārijiem, regulatīvi tehnisko standartu projekts būtu jāizstrādā augstākā (vispārīgākā), nevis detalizētā līmenī" *(European Banking Authority, 2016)*.

Līdz ar to, lai Regula 2018/389 sniedz zināmu skaidrojumu attiecībā uz drošu lietotāju autentificēšanu, tomēr ir jāņem vērā attiecīgā normatīvā akta izstrādātāja mērķis – vispārīgi skaidrot drošu lietotāju autentificēšanu, lai tas neapdraudētu tehnoloģisko neitralitāti, tādā veidā, apdraudot iespēju izmantot jaunus tehnoloģiskos risinājumus drošai lietotāju autentificēšanai.

2019. gada 21. jūnijā Eiropas Banku iestāde publicē viedokli par drošu lietotāju autentificēšanu, kurā skaidro atsevišķus elementus *(European Banking Authority, 2019)*. Attiecībā uz elementu "neatņemamas īpašības" norāda, ka: "Neatņemamas īpašības var ietvert uzvedības biometriju, kas identificē konkrēto autorizēto lietotāju. Eiropas Banku iestāde uzskata, ka iedzimtība, kas ietver bioloģisko un uzvedības biometrisko informāciju, attiecas uz ķermeņa daļu fizikālajām īpašībām, ķermeņa radītajām fizioloģiskajām īpašībām un uzvedības procesiem, kā arī uz jebkuru to kombināciju. Turklāt jebkuras uz neatņemamu īpašību pieejas ieviešana (tās kvalitāte) nosaka, vai tā ir vai nav atbilstoša neatņemamas īpašības elementam. Neatņemama īpašība ir elementa kategorija, kas ir visnovatoriskākā un ar visstraujāko attīstību, un tirgū nepārtraukti ienāk jaunas pieejas. Neatņemama īpašība var ietvert acs tīklenes un varavīksnenes skenēšanu, pirkstu nospiedumu skenēšanu, vēnu atpazīšanu, sejas un rokas ģeometrija (lietotāja sejas / rokas formas noteikšana), balss atpazīšana, taustiņa nospiešana dinamika (lietotāja identificēšana pēc rakstīšanas uz tastatūras un vilkšanas *(swiping)* veida, dažreiz tiek dēvēta par *astyping* un vilkšanas (swiping) modeļi) lenķis, kādā maksājuma pakalpojuma lietotās tur ierīci un maksājuma pakalpojuma lietotāja sirdsdarbības ātrums (unikāli identificējot maksājuma pakalpojuma lietotāju [..]"*(European Banking Authority, 2019)*.

No minētā secināms, ka elements "neatņemama īpašība" raksturo konkrētas fiziskās personas iedzimtas īpašības, kas dzīves laikā visbiežāk nemainās. "Neatņemama īpašība" var būt gan fizioloģiskas īpašības, gan īpašības, kas izriet no noteiktiem ieradumiem, piemēram, veida, kādā persona spiež taustiņus savā mobilajā telefonā, kā arī kā tur savu viedierīci. Šī elementa apstrāde ir saistīta ar personas datu apstrādi.

Attiecībā uz elementu "valdījums" Eiropas Banku iestāde savā viedoklī norāda, ka "ticami līdzekļi valdījuma apstiprināšanai, ģenerējot vai saņemot ierīcē dinamisku validācijas elementu" varētu būt vienreizējas paroles ģenerēšana, marķieris, īsziņa vai nospiežams paziņojums. Īsziņu gadījumā gan ir norādīts, ka īpašumtiesību elements nav pati īsziņa, bet gan parasti SIM karte, kas ir saistīta ar attiecīgo mobilā telefona numuru. Vienlaikus Eiropas Banku iestāde norāda, ka uz kartes *(European Banking Authority, 2019)*.

Līdz ar to nepietiek, ka personas valdījumā ir kāda ierīce, sniedzot maksājumu pakalpojumu, maksājumu pakalpojumu sniedzējam ir jāgūst pārliecība, ka šī ierīce ir šīs personas valdījumā, piemēram, nosūtot īsziņu uz mobilo telefonu, kuras saņemšanu personai ir jāapstiprina. Jānorāda, ka "valdījuma" elements neizslēdz pats par sevi iespējamību, ka ierīce atrodas citas personas valdījumā un validācijas elementu apstiprina šī cita persona.

Savukārt attiecībā uz elementu "zināšanas" Eiropas Banku iestāde savā viedoklī norāda, ka: "zināšanas" var veidot šādi elementi; parole, PIN, uz zināšanām balstītas atbildes, iegaumēts pārvilkšanas ceļš, kartes dati un uz kartes uzdrukātais drošības kods nebūtu zināšanu elements *(European Banking Authority, 2019)*.

Secināms, ka "zināšanas" ir noteikta informācija, kas ir zināma konkrētajam lietotājam, piemēram, parole, kā arī tādi jautājumi kā "mājdzīvnieka vārds" utt. Jānorāda, ka šīs zināšanas var nebūt unikālas, proti, arī citas personas var zināt atbildes uz zināšanās balstīties jautājumiem, piemēram, personas radinieki varētu zināt mājdzīvnieka vārdu, līdz ar to šis elements neizslēdz iespēju, ka autentifikāciju veic cita persona.

Kā norādīts iepriekš, tad elementi "valdījums" un "zināšanas" paši par sevi neapliecina to, ka tiek autentificēta konkrētā persona. Elements "neatņemamas īpašības" būtu uzskatāms par elementu ar augstāku ticamības pakāpi, ka tiek autentificēta īstā persona. Vienlaikus jānorāda uz apstākli, ka elements "neatņemamas īpašības" lielākoties varētu būt saistīts ar personas datu apstrādi, tādējādi radot maksājumu pakalpojumu sniedzējam paaugstinātu atbildību par personas datu apstrādi. Jebkurā gadījumā, kā norādīts iepriekš, tad maksājumu pakalpojumu sniedzējam ir pienākums piemērot vismaz divus no trim drošās lietotāja autentifikācijas elementiem. Lai arī Otrā maksājumu pakalpojumu direktīva it kā ļauj brīvi izvēlēties autentifikācijas elementus, tomēr Otrās maksājumu pakalpojumu direktīvas ievadapsvērumu 96. punkts paredz, ka drošības pasākumiem būtu jāatbilst ar maksājumu pakalpojumu saistītā riska līmenim. Līdz ar to maksājumu pakalpojumu sniedzējam ir jāizvērtē ar maksājumu pakalpojumu saistītais risks un jāpiemēro tam atbilstoši drošības pasākumi, tostarp attiecībā uz drošu lietotāja autentifikāciju. Par riskam neatbilstošu drošības pasākumu varētu tikt uzskatīts tāds maksājuma pakalpojums, kas ļautu brīvi pieslēgties personas konta, tikai iegūstos personas viedierīci.

Kad ir veicama droša lietotāja autentifikācija?

Saskaņā ar Otrās maksājumu pakalpojumu direktīvas 97. panta pirmo daļu - Dalībvalstis nodrošina, lai maksājumu pakalpojumu sniedzējs piemērotu drošu klienta autentificēšanu, kad maksātājs:

1) piekļūst savam maksājumu kontam tiešsaistē;
2) iniciē elektronisku maksājumu darījumu;
3) veic kādu darbību, izmantojot attālinātu kanālu, kas varētu ietvert ar maksājumiem saistītas krāpšanas risku vai cita veida ļaunprātīgu rīcību *(Par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 2002/65/EK, 2009/110/EK un 2013/36/ES un Regulu (ES) Nr. 1093/2010 un atceļ Direktīvu 2007/64/EK, 2015, 97.p. 1.daļa)*.

No minētā secināms, ka droša lietotāja autentificēšana nav piemērojama pilnīgi visos gadījumos, kad personai tiek sniegts maksājumu pakalpojums. Droša lietotāja autentifikācija ir piemērojama visos tajos gadījumos, kad maksātājs veic kādas darbības, izmantojot modernās tehnoloģijas – tiešsaiste, elektronisks maksājums vai attālināts kanāls.

Vienlaikus Otrā maksājumu pakalpojumu direktīva paredz arī specifiskus nosacījumus attiecībā uz atsevišķām darbībām, piemēram, attiecībā uz elektronisku maksājumu darījumu iniciēšanu, dalībvalstis attiecībā uz elektroniskiem attālinātiem maksājumu darījumiem nodrošina to, ka maksājumu pakalpojumu sniedzēji piemēro drošu klienta autentificēšanu, kas ietver elementus, kuri darījumu dinamiski sasaista ar konkrētu summu un konkrētu maksājuma saņēmēju *(Par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 2002/65/EK, 2009/110/EK un 2013/36/ES un Regulu (ES) Nr. 1093/2010 un atceļ Direktīvu 2007/64/EK, 2015, 97.p. 2.daļa)*. Minētais nozīmē, ka personai ir jāgūst pārliecība, ka iecerētā summa un pieprasītā summa sakrīt.

Secinājumi

Apkopojot iepriekš minēto, autore izdara šādus secinājumus

1. Otrās maksājumu pakalpojumu direktīvas viens no mērķiem ir sekmēt tehnoloģiju attīstību maksājumu pakalpojumu jomā, kas cita starpā tiek panākts ar "tehnoloģiski neitrālu" pieeju maksājumu pakalpojumiem, kas tostarp ir attiecināms arī uz drošu lietotāju autentifikāciju.
2. Droša lietotāju autentifikācija ietver trīs elementus: zināšanas, kas ietver informāciju, kuru zina konkrētais lietotājs, kas, piemēram, ir parole, valdījums, kas ir ierīce, kurai ir jāatrodas lietotāja valdījumā un maksājumu pakalpojumu sniedzējam ir jāiegūst apliecinājums par to, ka šī ierīce tiešām atrodas konkrētās personas valdījumā un neatņemama īpašība, kas ir personai raksturīga fizioloģiska vai ar konkrētiem ieradumiem saistīta īpašība.
3. Maksājumu pakalpojumu sniedzējam ir pienākums piemērot vismaz divus no trim iepriekš minētajiem drošas lietotāju autentifikācijas elementiem, izvērtējot sniegtā maksājumu pakalpojuma risku.
4. Droša lietotāju autentifikācija nav piemērojama visos gadījumos, kad lietotājam tiek sniegts maksājumu pakalpojums, bet šāda autentifikācija ir piemērojama gadījumos, kad maksātājs veic kādas darbības, izmantojot modernās tehnoloģijas – tiešsaiste, elektronisks maksājums vai attālināts kanāls.

Izmantotie avoti un literatūra

1. *Ar ko Eiropas Parlamenta un Padomes Direktīvu (ES) 2015/2366 papildina attiecībā uz regulatīvajiem tehniskajiem standartiem par drošu lietotāja autentificēšanu un vienotiem un drošiem atklātiem saziņas standartiem* (27.11.2017). Eiropas Savienības Komisijas deleģētā regula (ES) 2018/389, red. uz 22.04.2021. https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX%3A32018R0389, sk. 22.04.2021.
2. *Par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 2002/65/EK, 2009/110/EK un 2013/36/ES un Regulu (ES) Nr. 1093/2010 un atceļ Direktīvu 2007/64/EK* (25.11.2015). Eiropas Parlamenta un Padomes direktīva (ES) 2015/2366, red. uz 22.04.2021. https://eur-lex.europa.eu/legal-content/lv/TXT/?uri=CELEX%3A32015L2366, sk. 22.04.2021.
3. Eiropas Komisija (24.07.2013). *Priekšlikums Eiropas Parlamenta un Padomes Direktīva par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 2002/65/EK, 2013/36/ES un 2009/110/EK un atceļ Direktīvu 2007/64/EK* https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:52013PC0547, sk. 22.04.2021.
4. European Banking Authority (12.08.2016). *Consultation Paper On the draft Regulatory Technical Standards specifying the requirements on strong customer authentication and common and secure communication under PSD2*. Retrieved 22.04.2021 from: https://www.eba.europa.eu/sites/default/documents/files/ documents/10180/1548183/679054cf-474d-443c-9ca6-c60d56246bd1/Consultation%20Paper%20on%20 draft%20RTS%20on%20SCA%20and%20CSC%20%28EBA-CP-2016-11%29.pdf
5. European Banking Authority (21.06.2019). *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2*. Retrieved 22.04.2021 from: https://www.eba.europa.eu/sites/ default/documents/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/ EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf

Summary

The Second Payment Service Directive aims to promote technological development in the industry of payment services. To succeed it the "technologically neutral" approach for the payment services is applied. The "technologically neutral" approach must be applied also to strong customer authentication.

The Second Payment Services Directive requires payment service providers to apply secure customer authentication, which means that for the customer authentication shall be used for at least two elements: knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is).

The payment service provider is obliged to apply at least two of the above three elements of strong customer authentication when assessing the risk of the provided payment service.

Secure user authentication is not applicable in all cases when a payment service is provided to the user, but such authentication is applicable in cases where the payer performs any activities using modern technologies – online access to the account, electronic payment or remote channel.