მომხმარებლის ძლიერი ავთენტიფიკაციის წესთან მიმართებაში

კითხვები და მათზე პასუხები

***შენიშვნა:*** *დოკუმენტში მოცემული პასუხები ემსახურება წესის განმარტებას და ბაზრის მონაწილეების მიერ მისი დებულებების ერთგვარად გაგებას. დოკუმენტი მიზნად არ ისახავს წესთან შესაბამისობის შესაძლო ამომწურავი ჩამონათვალის ან/და ამომწურავი მაგალითების განსაზღვრას. გარკვეული განმარტებები შესაძლოა შეიცვალოს ბაზარზე დაფიქსირებული/იდენტიფიცირებული პრაქტიკიდან გამომდინარე. გარდა ამისა, შესაძლოა წესის კონკრეტული ჩანაწერი სასამართლოს მიერ განმარტებული იქნეს განსხვავებულად.*

**გავრცელების სფერო და გამონაკლისები**

|  |
| --- |
| 1. **როგორია წესის გავრცელების სფერო / რაზე ვრცელდება მისი მოქმედება?** |
| წესის პირველი მუხლის მე-3 პუნქტი განსაზღვრავს მოქმედების სფეროს. კერძოდ, ის ვრცელდება **გადამხდელის მიერ** განხორციელებულ სამ კატეგორიაში მოქცეულ ქმედებაზე:  ა) დისტანციურად ონლაინ რეჟიმში თავის საგადახდო ანგარიშზე წვდომაზე;  ბ) ელექტრონულ გადახდის ოპერაციის ინიციირებაზე;  გ) დისტანციური არხის საშუალებით განხორციელებულ ნებისმიერ ისეთ ქმედებაზე, რომელიც თაღლითობის ან/და სხვა უკანონო ქმედების რისკის მატარებელია;  **ამასთან, დამატებითი ინფორმაციისთვის:**  <https://eba.europa.eu/sites/default/documents/files/documents/10180/1303936/13129941-7581-4473-a767-52ec002bd00a/EBA-DP-2015-03%20%28RTS%20on%20SCA%20and%20CSC%20under%20PSD2%29.pdf?retry=1>  (მე-12 გვერდზე)  i. with regard to (a) above (პირველი მუხლის მე-3 პუნქტის „ა“ ქვეპუნქტისთვის), online access to payment accounts would cover all services where a PSU is using a device (e.g. PC, mobile device8, chip card, ATM) to log into the payment account for to retrieve information on the payment account. Online in this respect is understood as establishing a connection facilitating the message exchange between the device and the network hosting the payment account information for example via internet or telecommunication.  ii. with regard to (b) above (პირველი მუხლის მე-3 პუნქტის „ბ“ ქვეპუნქტისთვის), the initiation of electronic payment transactions would cover all payment transactions within the scope of PSD2 (such as card payments, credit transfers, e-money transactions, direct debits), except where the payment instruction is not electronic (such as physical mail-order, paper based credit transfer or paper based direct debits or telephone orders).  iii. with regard to (c) above (პირველი მუხლის მე-3 პუნქტის „გ“ ქვეპუნქტისთვის), actions carried out via a remote channel that may imply a risk of payment fraud or other abuses could be clarified as covering all actions intrinsically linked to payment services not covered in the categories (a) and (b) above. This could for example include actions related to the activation and deactivations of payment functionalities, the amendment of trusted beneficiaries (“white lists”) - or blocked beneficiaries (“black-lists”), the setting of limits or the generation of virtual cards or changing PSU data that may imply a risk of payment fraud or other abuses. It only includes actions that are conducted via the internet or through a device that can be used for distance communication (e.g. mobile devices). |

|  |
| --- |
| 1. **გადახდის ოპერაციას როგორ განმარტავთ და თუ იქნება სწორი N8/04 ბრძანების დეფინიციებით რომ განვმარტოთ?**   საკრედიტო გადახდის ოპერაცია (საკრედიტო გადარიცხვა) − გადამხდელის მიერ ინიციირებული ფულადი სახსრების გადარიცხვის ოპერაცია; სადებეტო გადახდის ოპერაცია (სადებეტო გადარიცხვა) - მიმღების მიერ ინიციირებული გადამხდელის ანგარიშიდან ფულადი სახსრების გადარიცხვის ოპერაცია. ასევე, საქართველოს კანონმდებლობით შესაბამისი უფლებებით აღჭურვილი პირის მიერ ინიციირებული გადამხდელის ანგარიშიდან ფულადი სახსრების გადარიცხვის ოპერაცია, გარდა იმ შემთხვევებისა, სადაც ეს პირი მოქმედებს როგორც გადამხდელი. |
| „გადახდის ოპერაციის“ განმარტება მოცემულია „საგადახდო სისტემისა და საგადახდო მომსახურების შესახებ“ საქართველოს კანონში (გადახდის ოპერაცია − გადამხდელის ან მიმღების მიერ ინიციირებული ფულადი სახსრების განთავსების/ჩარიცხვის, გადარიცხვის ან გატანის ოპერაცია).  წესის მოქმედების სფეროდან გამომდინარე, ძლიერი ავთენთიფიკაციის მოთხოვნა ვრცელდება **გადამხდელის მიერ** გადახდის ოპერაციის **ინიციირებაზე**  (წესის პირველი მუხლის მე-3 პუნქტის „ბ“ ქვეპუნქტი).  **პირდაპირ დებეტზე** და ბარათით განხორციელებულ გარკვეულ ოპერაციებზე (‘card payments initiated by the payee only’), სადაც გადამხდელს წინასწარ გაცემული აქვს **მანდატი** მიმღებზე, ძლიერი ავთენთიფიკაციის მოთხოვნა არ არის სავალდებულო.  მანდატის გაცემა ძლიერი ავთენთიფიკაციით უნდა მოხდეს.  იხ. დეტალური ინფორმაცია ბმულზე:  <https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4031> |

|  |
| --- |
| 1. **ვრცელდება თუ არა წესი მომხმარებლის მიერ ბანკის/პროვაიდერის სერვის ცენტრებში ბანკის/პროვაიდერის თანამშრომლის შესრულებულ ოპერაციებზეც?** |
| წესი არ ვრცელდება არაელექტრონული ფორმით გაცემულ დავალებებზე.  *the payment instruction is not electronic (such as physical mail-order, paper based credit transfer or paper based direct debits or telephone orders).*  <https://eba.europa.eu/sites/default/documents/files/documents/10180/1303936/13129941-7581-4473-a767-52ec002bd00a/EBA-DP-2015-03%20%28RTS%20on%20SCA%20and%20CSC%20under%20PSD2%29.pdf?retry=1>  (მე-12 გვერდზე) |

|  |
| --- |
| 1. **წესის მოთხოვნები უნდა გავავრცელოთ თუ არა სატელეფონო სერვის ცენტრის მომსახურების პროცესზე?** |
| წესი არ ვრცელდება ტელეფონისა და ელექტრონული ფოსტის საშუალებით ინიციირებულ ოპერაციებზე (ე.წ. MO-TO ოპერაციები). შესაბამისად, წესი არ ვრცელდება სატელეფონო სერვის ცენტრის მომსახურებაზე.  იხილეთ პირველი და მე-2 კითხვის პასუხები. |

|  |
| --- |
| 1. **ეხება თუ არა წესი ელექტრონული ფულის პროვაიდერებს?** |
| დიახ. |

|  |
| --- |
| 1. **ვრცელდება თუ არა წესი ნებისმიერი ბარათით ჩატარებულ ნებისმიერ ოპერაციაზე?** |
| წესი ვრცელდება გადამხდელის მიერ ინიციირებულ საბარათე გადახდის ოპერაციებზეც.  **საბარათე ოპერაციებზე დეტალური განმარტება იხილეთ ამ ბმულზე:**  <https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4031>  გვერდი 20. პუნქტი 7.3-დან  <https://eba.europa.eu/documents/10180/855014/EBA-CP-2014-31+%28CP+on+security+of+internet+payments%29.pdf> |

|  |
| --- |
| 1. **ძლიერი ავთენტიკაციის მოთხოვნები თუ ვრცელდება პოს-ტერმინალზე, ბარათბზე და ბანკომატებზე?** |
| დიახ.  **საბარათე ოპერაციებზე დეტალური განმარტება იხილეთ ამ ბმულზე:**  <https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4031> |

|  |
| --- |
| 1. **ვრცელდება თუ არა აღნიშნული წესი ბარათით ოფლაინ გადახდების შემთხვევაში (მაგ: თვითმფრინავში გადახდა)?** |
| დიახ, ე.წ. ოფლაინ რეჟიმში გადახდებზეც ვრცელდება. იხილეთ EBA-ს განმარტება აღნიშნულთან დაკავშირებით:  Article 97(1)(b) of Directive 2015/2366/EU (PSD2) prescribes that the payment service provider (PSP) shall apply ‘strong customer authentication (SCA) where the payer initiates an electronic payment transaction’.  Therefore, in the case where the payer initiates an electronic card-based payment transaction at a Point of Sale (POS) in offline mode or through a remote channel (the internet), the issuer shall apply Strong Customer Authentication (SCA) to that transaction, unless an exemption from SCA applies in accordance with Articles 11– 18 of the Delegated Regulation (EU) 2018/389. Other exemptions from SCA to those specified within the Delegated Regulation are not available.  With regard to remote electronic transactions, Articles 4 and 5 of the Delegated Regulation also apply.  In that regard, the specific case described above with a closed wireless network that does not have internet connectivity and does not use a POS terminal, may not allow SCA to be applied.  In the case where the airplane is equipped with a POS terminal working in offline mode, the payer may be able to initiate an electronic card-based payment transaction and subsequently apply SCA. As clarified in Q&A 2018\_4055, the PIN can be transmitted and verified offline, provided that it meets the requirements of Articles 6(1), 22(1) and 22(4) of the Delegated Regulation.  Question ID:2019\_4740  <https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4740> |

|  |
| --- |
| 1. **ეს წესი ანონიმურ ინსტრუმენტებზე ვრცელდება?** |
| არ ვრცელდება. თუმცა, თუ მომხმარებელი დაიდენტიფიცირდება, მასზე უნდა გავრცელდეს ძლიერი ავთენტიფიკაციის წესი.  გთხოვთ, იხილოთ ამონარიდი ევრორეგულაციიდან (EU) 2018/389:  „(8) Due to their very nature, payments made through the use of an anonymous payment instruments are not subject to the obligation of strong customer authentication. Where the anonymity of such instruments is lifted on contractual or legislative grounds, payments are subject to the security requirements that follow from Directive (EU) 2015/2366 and this Regulatory Technical Standard.“ |

|  |
| --- |
| 1. **სასტუმროებში გადახდები ხშირად ასეთი სქემით ხდება: თავდაპირველად, სანამ კლიენტი ჩავა სასტუმროში, ხდება პრეავტორიზაცია (ბარათის ინფორმაცია გადაეცემა ტელეფონით, მეილით და ა.შ), ანუ თანხა იბლოკება კლიენტის ბარათზე (დაბლოკვა ხდება პოს ტერმინალიდან). შემდეგ კლიენტი ჩადის სასტუმროში და მაგ დროს ხდება თანხის ჩამოჭრა. ვრცელდება თუ არა წესი ამ ტიპის გადახდებზე?** |
| სავაჭრო/მომსახურების ობიექტის (მიმღების) მიერ ინიციირებულ ოპერაციებზე არ ვრცელდება წესის მოქმედება. ხოლო, თუ ოპერაცია მომხმარებლის მიერ არის ინიციირებული, სავაჭრო/მომსახურების ობიექტს უნდა ჰქონდეს მომხმარებლის თანხმობა. თუმცა, აღნიშნული დამოკიდებულია სხვადასხვა გარემოებებსა და შემთხვევებზე. გთხოვთ, იხილოთ დოკუმენტები ქვემოთ მოცემულ ბმულებზე.  <https://www.visa.co.uk/dam/VCOM/regional/ve/unitedkingdom/PDF/sca/Visa%20SCA%20Guide%20Travel%20%20Hospitality%20v1.1%2011-03-19.pdf>  <https://www.visa.es/dam/VCOM/regional/ve/unitedkingdom/PDF/sca/Visa_PSD2_SCA_Implementation_Guide.pdf> |

|  |
| --- |
| 1. **თუ ბარათისა და პინკოდის გამოყენება ხდება ტერმინალზე მომხმარებლის მხოლოდ იდენტიფიკაცია/ვერიფიკაციის მიზნებისთვის, აღნიშნულ შემთხვევაზე წესი ვრცელდება?** |
| წესი არ ვრცელდება მომხმარებლის იდენტიფიკაციასა და ვერიფიკაციის პროცედურებზე. |

|  |
| --- |
| 1. **თუ მომხმარებელი ანგარიშზე არსებულ ნაშთს იგებს SMS ბანკინგის გამოყენებით, საჭიროა ძლიერი ავთენტიფიკაციის განხორციელება? (ანუ მომხმარებელი აგზავნის ფიქსირებულ ნომერზე სპეციალურ კოდს და ეგზავნება აღნიშნული ინფორმაცია SMS-ით).** |
| წესის მოქმედება არ ვრცელდება მოკლე ტექსტური შეტყობინებით (SMS) ინფორმაციის მოთხოვნაზე, ვინაიდან აღნიშნული არ მიმდინარეობს ონლაინ რეჟიმში. ამასთან კავშირში, გთხოვთ, იხილოთ EBA-ს მოსაზრება:  „In the EBA’s view, mail and telephone orders are out of the scope of the principle of SCA under PSD2 and therefore not subject to the RTS requirements.“ [გვ. 73, EBA/RTS/2017/02, 23 February 2017]. |

|  |
| --- |
| 1. **შესაძლებელია თუ არა, არ გამოვიყენოთ მომხმარებლის ძლიერი ავთენთიფიკაცია პირდაპირ დებეტში და მუდმივ დავალებაში (“standing order”-ში) შემავალი ყველა მომდევნო გადახდის ოპერაციის ინიცირებისთვის, თუ განმეორებადი/პერიოდული გადახდის ოპერაციის მიმღები უცვლელია და თანხა არ აღემატება იმ ლიმიტს, რაც კლიენტმა დაგვიდასტურა ძლიერი ავთენტიფიკაციით პირდაპირი დებეტის და მუდმივი დავალების რეგისტრაციისას?** |
| **პირდაპირი დებეტი** არის მიმღების მიერ ინიციირებული ოპერაცია, რაზეც არ ვრცელდება წესი. რაც შეეხება, ე.წ. „პირდაპირი დებეტის რეგისტრაციას“, აუცილებელია ძლიერი ავთენტიფიკაციის გამოყენება. აღნიშნულის ფარგლებში შემდგომი გადახდები არ საჭიროებს ძლიერ ავთენტიფიკაციას.  საყოფაცხოვრებო (კომუნალური) გადახდებისთვის იხილეთ წესის 31-ე მუხლის (გარდამავალი დებულებები) მე-8 პუნქტი.  განმეორებად/პერიოდულ გადახდის ოპერაციებთან მიმართებაში, გთხოვთ, იხილოთ წესის მე-16 მუხლი. |

|  |
| --- |
| 1. **ვრცელდება თუ არა წესი ისეთი „recurring“ ტიპის საბარათე გადახდებზე, როცა მომხმარებელი ამატებს ბარათს და შემდეგ მერჩანტი ახორციელებს რეგულარულად თანხის ჩამოჭრას ავტომატურ რეჟიმში?**   **ამ შემთხვევაში ეს არ ჩაითვლება როგორც „არა კლიენტის მიერ ინიცირებული გადახდა“ და წესი არ გავრცელდება?** |
| როდესაც პირველად მიღებული თანხმობის საფუძველზე მერჩანტი ახორციელებს ინიციირებას, ამ უკანასკნელზე არ გავრცელდება წესის მოქმედება. თუმცა, მომხმარებლის თანხმობა გაცემული უნდა იყოს ძლიერი ავთენტიფიკაციის საფუძველზე. |

|  |
| --- |
| 1. **როდესაც ოპერაციის გადახდა ხორციელდება თვითმომსახურების კიოსკის გამოყენებით, ნაღდი ფულით ან საგადახდო ბარათით (ბარათით გადახდა ხორციელდება ისევე როგორც პოს ტერმინალიდან), ითვლება თუ არა ეს ელექტრონულ ოპერაციად და ვრცელდება თუ არა ძლიერი იდენტიფიკაციის განხორციელების მოთხოვნები?** |
| თუ ნაღდი ფულით ხდება გადახდა, მაშინ მასზე არ ვრცელდება წესის მოქმედება.  პოს-ტერმინალის საშუალებით ბარათით გადახდაზე ვრცელდება წესის მოქმედება. შესაბამისად, თუ თვითმომსახურების კიოსკით გადახდა პოს-ტერმინალით გადახდის ანალოგიურია, მასზე გავრცელდება წესის მოქმედება. |

|  |
| --- |
| 1. **ცალსახად ბანკმა/პროვაიდერმა უნდა განსაზღვროს პირველი მუხლის მე-3 პუნქტის „გ“ ქვეპუნქტში გათვალისწინებული ქმედებები?** |
| დიახ, აღნიშნულს განსაზღვრავს ბანკი/პროვაიდერი.    actions carried out via a remote channel that may imply a risk of payment fraud or other abuses could be clarified as covering all actions intrinsically linked to payment services not covered in the categories (a) and (b) above. This could for example include actions related to the activation and deactivations of payment functionalities, the amendment of trusted beneficiaries (“white lists”) - or blocked beneficiaries (“black-lists”), the setting of limits or the generation of virtual cards or changing PSU data that may imply a risk of payment fraud or other abuses. It only includes actions that are conducted via the internet or through a device that can be used for distance communication (e.g. mobile devices).  EBA Discussion Paper, EBA/DP/2015/03, გვ. 11-12, პუნქტი 27 (iii), <https://eba.europa.eu/documents/10180/1303936/EBA-DP-2015-03+%28RTS+on+SCA+and+CSC+under+PSD2%29.pdf>  ჩანაწერი მიუთითებს ისეთ ქმედებებზე, რომელიც თაღლითობის ან/და სხვა უკანონო ქმედების რისკის მატარებელია. ერთიდაიგივე ქმედება შესაძლოა რისკის შემცველი იყოს ერთი პროვაიდერის ჭრილში, ხოლო მეორე პროვაიდერთან - არა. |

|  |
| --- |
| 1. **„ავთენტიფიკაცია“-ს ტერმინის (2.ა.) განმარტების მიხედვით, მოთხოვნა ვრცელდება ინტერნეტ-ბანკინგში შესვლის პროცესზე, თუმცა ძლიერი ავთენტიფიკაციის მოთხოვნები ვრცელდება ტრანზაქციის დადასტურებაზეც (როგორც ეს შემდგომი მოთხოვნებიდან ჩანს). შესაბამისად, განმარტებას უნდა დაემატოს ეს ნაწილიც.** |
| ტერმინის განმარტებაში არ არის დაკონკრეტებული თუ რა პროცესზე ვრცელდება იგი. ტერმინის განმარტება მოცემულია ზოგადი შინაარსის სახით.  *„ავთენტიფიკაცია - პროცედურა, რომელიც საგადახდო მომსახურების პროვაიდერს საშუალებას აძლევს მოახდინოს მომხმარებლის იდენტობის დადგენა ან/და საგადახდო ინსტრუმენტის გამოყენების ვალიდურობის დადგენა, რომელიც მათ შორის, მოიცავს მომხმარებლის მიერ გამოყენებული უსაფრთხოების პერსონალიზებული მახასიათებლების შემოწმებას.“*  p.s. აღნიშნული განმარტება ოდნავ განსხვავდება ამჟამად „საგადახდო სისტემისა და საგადახდო მომსახურების“ კანონის განმარტებისგან, თუმცა იგეგმება კანონში ცვლილებების განხორციელება (წესის ტერმინი PSD2-ის განმარტების შესაბამისია). |

|  |
| --- |
| 1. **იდენტობის დადგენა სპეციფიური და ახალი ტერმინია, რაც გაუგებრობას ქმნის. შთაბეჭდილება იქმნება რომ იდენტიფიკაციის ალტერნატიულ ტერმინთან გვაქვს საქმე, რაც დისტანციურ პროცესებში შესრულებადობას აპრობლემებს. დისტანციურ არხებში მომხმარებლის ზუსტი იდენტობის დადგენა მხოლოდ ბიომეტრიული მონაცემით იქნება შესაძლებელი, ისიც არა 100 %-იანი სიზუსტით. შესაბამისად, ტერმინი დაზუსტებას საჭიროებს, რომ იდენტიფიკაციის პროცესთან გაიგივება არ მოხდეს.** |
| „იდენტობის დადგენა“ შესაბამისია PSD2-ის განმარტების შესაბამის ფრაზასთან „verify identity of the payment service user”.  ‘authentication’ means a procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user’s personalised security credentials;  მომხმარებლის „იდენტიფიკაცია“ საჭიროა მომხმარებელთან საქმიანი ურთიერთობის დამყარებისას. „აუთენთიფიკაცია“ საჭიროა „იდენტიფიცირებული“ მომხმარებლის ამოცნობისთვის. |

|  |
| --- |
| 1. **მაგნიტურ-ზოლიანი ბარათის გამოყენების შემთხვევაში, შეიძლება ძლიერი ავთენტიფიკაცია მოხდეს ფლობის ელემენტის გამოყენების გარეშე. ე.ი. რადგან ბარათი ვერ გამოიყენება დინამიური კოდის გენერირებისთვის, შეიძლება მაინც გამოიყენოს მომხმარებელმა მაგნიტურ-ზოლიანი ბარათი, თუმცა ავთენტიფიკაცია მოხდეს დანარჩენი ელემენტებით (ან ფლობის სხვა ელემენტით, გარდა ბარათის ფლობისა)?** |
| ზოგადად, მაგნიტურ-ზოლიანი ბარათი, მათ შორის, უსაფრთხოების კუთხით, ვერ აკმაყოფილებს წესის მოთხოვნებს. შესაბამისად, ასეთი ბარათი ვერ იქნება გამოყენებული ვერცერთ შემთხვევაში. თუ ბარათი დააკმაყოფილებს სპეციფიკური და შეზღუდული გამოყენების საგადახდო ინსტრუმენტების მიმართ განსაზღვრულ მოთხოვნებს, წესი მასზე არ გავრცელდება. აღნიშნულთან მიმართებაში, გთხოვთ, იხილოთ წესის მე-4 მუხლი. |

|  |
| --- |
| 1. **თუ მომხმარებელს აქვს მაგნიტურ-ზოლიანი ბარათი , შეიძლება თუ არა მასზე რამე გამონაკლისი დაემატოს?** |
| წესში (მე-4 მუხლი) გათვალისწინებულია დებულებები, რომლებიც ეხება სპეციფიკურ და შეზღუდული გამოყენების საგადახდო ინსტრუმენტებს. მათზე არ გავრცელდება წესის მოქმედება კრიტერიუმების დაკმაყოფილების შემთხვევაში. პროვაიდერს შეუძლია საქართველოს ეროვნულ ბანკს წერილობით წარუდგინოს ინსტრუმენტის შესახებ ინფორმაცია და აღწერა. ამის საფუძველზე და შესაბამისობის შემთხვევაში აღნიშნული უფლებამოსილებით სარგებლობის თაობაზე გადაწყვეტილებას იღებს სებ-ი. |

|  |
| --- |
| 1. **რას ნიშნავს ჩანაწერი - ინსტრუმენტი შესაძლოა გამოყენებული იქნეს მხოლოდ საქონლის ან მომსახურების მკაცრად შეზღუდული სპექტრის შესაძენად?** |
| აღნიშნული შინაარსი ეხება სპეციფიკური და შეზღუდული გამოყენების საგადახდო ინსტრუმენტების შესახებ გამონაკლისს (მე-4 მუხლი). შეუძლებელი უნდა იყოს ინსტრუმენტის სრულფასოვნად გამოყენება. მომხმარებელს უნდა შეეძლოს მხოლოდ განსაზღვრული და მკაცრად ლიმიტირებული რაოდენობის საქონლის ან/და მომსახურების შეძენა.  წესის თანახმად, ასეთი ინსტრუმენტების წესის მოქმედების სფეროდან გამორიცხვა ხდება სებ-ისთვის აღწერის წერილობით წარდგენისა და ყოველი კონკრეტული შემთხვევისთვის მის მიერ გადაწყვეტილების მიღების საფუძველზე. |

# **ავთენტიფიკაციის ელემენტები და ავთენტიფიკაციის კოდი**

|  |
| --- |
| 1. **რა მოიაზრება ცოდნა, ფლობა და უნიკალურობაში?** |
| გთხოვთ, აღნიშნული სამივე კატეგორიის ელემენტების ვრცელი განმარტებისთვის გაეცნოთ EBA-ს მოსაზრებებს ელემენტებთან მიმართებაში. თუმცა გასათვალისწინებელია, რომ როგორც ამ დოკუმენტშია აღნიშნული, მასში მოცემული ელემენტების ჩამონათვალი ამომწურავი არ არის.  <https://eba.europa.eu/documents/10180/2622242/EBA+Opinion+on+SCA+elements+under+PSD2+.pdf> |

|  |
| --- |
| 1. **ელემენტების რა კომბინაცია ჩაითვლება ძლიერ ავთენტიფიკაციად?** |
| მხოლოდ ერთი კატეგორიის ელემენტით/ელემენტებით ავთენტიფიკაცია არ არის ძლიერი ავთენტიფიკაცია. თუმცა, სხვა კატეგორიის ელემენტებთან ერთობლიობაში ჩაითვლება ძლიერ ავთენთიფიკაციად.  EBA-ს დოკუმენტიში მოცემულია სამივე კატეგორიის ელემენტების ჩამონათვალი. სხვადასხვა კატეგორიის ცხრილებიდან აღებული ელემენტების კომბინაცია ქმნის ძლიერი ავთენტიფიკაციის მექანიზმს.  <https://eba.europa.eu/documents/10180/2622242/EBA+Opinion+on+SCA+elements+under+PSD2+.pdf> |

|  |
| --- |
| 1. **სანდო მოწყობილობის განმარტების შემოტანა არ განიხილება?** |
| ავთენტიფიკაციისთვის შესაძლოა გამოყენებული იყოს „ფლობის“ კატეგორიის ელემენტები. თუ პროვაიდერი განიხილავს რომელიმე მოწყობილობის „ფლობის“ ელემენტად გამოყენებას, მას უნდა ჰქონდე რწმუნება, რომ აღნიშნული მოწყობილობა ეკუთვნის მომხმარებელს. განსაკუთრებული ყურადღება უნდა მიექცეს მომხმარებლის მიერ პირველად გამოყენებულ მოწყობილობებს. |

|  |
| --- |
| 1. **ბარათის ნომერი და CVV კოდი არის თუ არა უსაფრთხოების პერსონიფიცირებული მახასიათებელი?** |
| ბარათზე ფიზიკურად დატანილი სტატიკური CVV და ბარათის ნომერი არ არის უსაფრთხოების პერსონიფიცირებული მახასიათებელი.  თუმცა, თუ ეს ინფორმაცია ელექტრონულია ან/და CVV არის ცვალებადი, მაშინ ისინი წარმოადგენს უსაფრთხოების პერსონიფიცირებულ მახასიათებლებს.  „The EBA Opinion on the Implementation of the RTS stated that the card details and security code printed on the card would not constitute a knowledge element. In addition, while a card with a dynamic card security code may constitute a possession element, it would not constitute a knowledge element. That being said, in the event, for instance, that the card security code was not printed on the card and was sent separately to the PSU, in the same way as a PSP may send a PIN for a new card, it could constitute a knowledge element. The same may apply to virtual cards (where the PSU receives a single-use digital card number and card security code).“.  <https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf>  EBA-Op-2019-06. 21 June 2019 |

|  |
| --- |
| 1. **„Fingerprint scanning“-ში თითის ანაბეჭდების პროვაიდერის მხარეს შენახვა იგულისხმება, თუ არსებულ ე.წ. „Device specific native“ გადაწყვეტას შეგვიძლია ვენდოთ?** |
| ტექნოლოგიური ნეიტრალიტეტის დაცვის მიზნით, წესი არ აკონკრეტებს ტექნოლოგიური გადაწყვეტის ტიპს. მნიშვნელოვანია, რომ კონკრეტული გადაწყვეტა იყოს სანდო და აკმაყოფილებდეს წესის მოთხოვნებს.  გთხოვთ, მოწყობილობასთან დაკავშირებით ასევე იხილოთ 23-ე კითხვა. |

|  |
| --- |
| 1. **Fingerprint/FaceID/Passcode-ით ავთენტიფიკაციის გავლისას მონაწილეობს მომხმარებლის მოწყობილობა (უნიკალობა და მოწყობილობა, ან ცოდნა და მოწყობილობა). აღნიშნული სახის ავთენტიფიკაცია დააკმაყოფილებს ძლიერი ავთენტიფიკაციის მოთხოვნებს. ხომ ასეა?** |
| თითის ანაბეჭდის/სახის ამოცნობის ელემენტის (ან პაროლი) და მოწყობილობაზე ჩაწერილი აპლიკაციის კომბინაცია აკმაყოფილებს წესის მოთხოვნებს. გასათვალისწინებელია, რომ აპლიკაცია დაკავშირებული უნდა იყოს კონკრეტულ მოწყობილობასთან და უნიკალურობის ელემენტიც (თითის ანაბეჭდი/სახის ამოცნობის ელემენტი) უნდა იყოს საიმედო.  გთხოვთ, მოწყობილობასთან დაკავშირებით ასევე იხილოთ 23-ე კითხვა. |

|  |
| --- |
| 1. **ელექტრონული გადახდების ოპერაციებისთვის რომელი სცენარები შეიძლება ჩაითვალოს ძლიერ ავთენტიფიკაციად? მაგალითად: ცოდნა - ინტერნეტ ბანკის User/Pass, ხოლო, ფლობა: SMS OTP.** |
| თქვენ მიერ ხსენებული კომბინაცია, ინტერნეტ ბანკის პაროლი და მობილურის ნომერზე გაგზავნილი ერთჯერადი კოდი, დააკმაყოფილებს წესის მოთხოვნას. გარდა ამისა, მაგალითისთვის, შესაძლებელია შემდეგი კომბინაციები:   * პაროლი და თითის ანაბეჭდი/სახის ამოცნობა ან სხვა ბიომეტრიული მონაცემები (უნიკალურობის კატეგორია); * ერთჯერადი კოდი და თითის ანაბეჭდი/სახის ამოცნობა ან სხვა.   წესი არ ზღუდავს არცერთი კომბინაციის გამოყენებას, იმ პირობით, რომ ორივე ელემენტი იქნება სხვადასხვა კატეგორიიდან.  გასათვალისწინებელია, რომ „მომხმარებლის დასახელება“ არ წარმოადგენს ავთენტიფიკაციის ელემენტს. |

|  |
| --- |
| 1. **გამარტივებული გადახდა პროვაიდერის საფულით - საფულეში შესაძლებელია პარამეტრებში გამარტივებული გადახდის დაყენება. ეს ნიშნავს, რომ 100 ლარამდე თანხებზე გადახდა შესაძლებელია ტელეფონის განბლოკვით (ანუ აქაც 2 ფაქტორია - მოწყობილობა და ბიომეტრია ან მოწყობილობა და პასკოდი) და ტერმინალზე მიდებით. 100 ლარზე ზემოთ თანხებზე კი საჭირო ხდება გადახდის გაკეთება აპლიკაციაში შესვლით. გთხოვთ დაგვიდასტუროთ, რომ გამარტივებული გადახდა აკმაყოფილებს წესის მოთხოვნებს.** |
| შესაძლებელია ასეთი მექანიზმის გამოყენება, თუ დაკმაყოფილდება უკონტაქტო გადახდების გამონაკლისის მოთხოვნები.  ასევე, გასათვალისწინებელია ავთენტიფიკაციის კოდთან დაკავშირებული მოთხოვნები. |

|  |
| --- |
| 1. **„Knowledge based challenge questions“-ში არის თუ არა კითხვების ფოტოებით ჩანაცვლება შესაძლებელი?** |
| თუ კითხვები ჩანაცვლებული იქნება ფოტოებით, გასათვალისწინებელია, რომ აღნიშნულმა არ შეასუსტოს კონკრეტული გადაწყვეტიდან გამომდინარე მომხმარებლის დაცულობის ხარისხი და, ასევე, არ მოხდეს თაღლითობის ან/და სხვა უკანონო ქმედების რისკის გაზრდა. სურათები მომხმარებლის მიერ თავიდანვე უნდა იქნეს არჩეული მნიშვნელოვნად ფართო ჩამონათვალიდან (ვარიანტებიდან), და გარდა ამისა, დაუშვებელია პროვაიდერის თანამშრომლებს წვდომა ჰქონდეს აღნიშნულ სურათებზე. |

|  |
| --- |
| 1. **EBA-ს განმარტებაში აღნიშნულია „Hand and face geometry“-ს გადაწყვეტის შესახებ. ხელის სკანერის გამოყენება აუცილებელია? სმარტფონის კამერის გამოყენება არ ჩაითვლება საკმარისად?** |
| ტექნოლოგიური ნეიტრალიტეტიდან გამომდინარე, პროვაიდერი უფლებამოსილია თავად აირჩიოს გამოსაყენებელი გადაწყვეტა, რომელიც უნდა იყოს საიმედო. |

|  |
| --- |
| 1. **გთხოვთ, განგვიმარტოთ ერთჯერადი კოდი (OTP) ფლობის ელემენტია, თუ ცოდნის?** |
| კოდი, რომელიც შეიძლება მობილურის ნომერზე გაიგზავნოს და არის ერთჯერადი, წარმოადგენს ფლობის კატეგორიის ელემენტს.  მნიშვნელოვანია, რომ მობილურის ნომერი ვერიფიცირებული იყოს წინაწარ პროვაიდერის მიერ. |

|  |
| --- |
| 1. **როგორც ვიცით OTP გენერირებული უნდა იყოს კონკრეტულ მიმღებზე და თანხაზე. რა ბედი ეწევა OTP-ს, რომელსაც მომხმარებლები იყენებენ ავტორიზაციისთვის?** |
| ერთჯერადი კოდი არ წარმოადგენს ავტენთიფიკაციის კოდს, არამედ არის ავთენთიფიკაციის ერთ-ერთი ელემენტი.  ანგარიშზე წვდომისათვის არ მოითხოვება ავთენტიფიკაციის კოდის დინამიური დაკავშირება მიმღებთან და თანხასთან. ეს სავალდებულოა მხოლოდ გადახდის ოპერაციის ინიციირებისას. |

|  |
| --- |
| 1. **ცვალებადი პასკოდი მიიჩნევა თუ არა ცოდნის ელემენტად?** |
| პასკოდი ჩაითვლება ცოდნის კარეგორიის ელემენტად, თუ ის მომხმარებელმა ანგარიშზე წვდომამდე/ინიციირებამდე იცის (ფასვორდის მსგავსად). |

|  |
| --- |
| 1. **მიიჩნევა თუ არა შემდეგი CVV ავთენტიფიკაციის ელემენტად: ბარათის შემთხვევაში ყოველ 3 წუთში ერთხელ შეცვლილი CVV კოდი?** |
| ბარათი, მასზე არსებული ცვალებადი CVV-ით ჩაითვლება ფლობის კატეგორიის ელემენტად. |

|  |
| --- |
| 1. **ელ კომერციის ტრანზაქციის დროს 3D კოდი რიგ შემთხვევებში არ/ვერ გენერირდება. მაგალითად ლოკალურ და UPI ბარათებზე.** |
| კლიენტის ძლიერი ავთენტიფიკაცია სავალდებულოა ყველა ტიპის ბარათებისთვის, როგორც ლოკალური, ასევე საერთაშორისო. მათზე ასევე, ვრცელდება წესით დადგენილი გამონაკლისები. |

|  |
| --- |
| 1. **შეგვიძლია დანამდვილებით ვთქვათ, რომ „3D secure version 2.2“ დანერგვის შემდეგ, ელექტრონული კომერციის არხში შესრულებული ტრანზაქციის დასადასტურებლად გაგზავნილი „3D secure“ კოდი დააკმაყოფილებს ძლიერი ავთენტიფიკაციის მოთხოვნას? თუ საჭიროა დამატებით სხვა კატეგორიის ელემენტის გამოყენებაც?** |
| EBA-ს მოსაზრების თანახმად, “3D secure version 2.2” უზრუნველყოფს SCA-სთან სრულ თავსებადობას. ასევე, მხოლოდ აღნიშნული კოდის გამოყენება არ წარმოადგენს ძლიერ ავტენტიფიკაციას. კოდი იგზავნება მობილურის ნომერზე, რაც ექცევა ფლობის კატეგორიაში. შესაბამისად, ძლიერი ავთენტიფიკაციისთვის საჭირო იქნება კიდევ ერთი კატეგორიის ელემენეტი (რომელიც არ იქნება ფლობის კატეგორიიდან). |

|  |
| --- |
| 1. **სწორი განმარტებაა თუ არა, რომ ტერმინალის შემთხვევაში, ჩიპის ფლობა და პინკოდის ცოდნა ჩაითვლება ორკომპონენტიან ავთენტიფიკაციად?** |
| დიახ. საბარათე ინფორმაციის წაკითხვა უნდა განხორციელდეს სპეციალური წამკითხველების საშუალებით (Card evidenced by a card reader) - ეს ფლობის კატეგორიის ელემენტად განიხილება. პინი ცოდნის კატეგორიის ელემენტია. |

|  |
| --- |
| 1. **ბარათი ფლობის კატეგრიის ელემენტად რომ ჩაითვალოს, საბარათე ინფორმაციის წაკითხვა უნდა განხორციელდეს სპეციალური წამკითხველის საშუალებით („Card evidenced by a card reader“). უკონტაქტო წამკითხველიც შეიძლება ჩაითვალოს ბარათის წამკითხველად (card reader)?** |
| უკონტაქტო წამკითხველი ჩაითვლება ე.წ. ბარათის წამკითხველად (card reader), თუ მისი საშუალებით ხდება სულ მცირე იმავე მონაცემების წაკითხვა, როგორც ამას ადგილი აქვს ბარათის პოს-ტერმინალში განთავსების შემთხვევაში. |

|  |
| --- |
| 1. **შეიძლება თუ არა პირადი ნომრის და პირადობის მოწმობის უნიკალური ნომრის კომბინაცია ჩაითვალოს ცოდნის კომპონენტად? პირადობის მოწმობის ნომერი არ არის გავრცელებული ინფორმაცია და ხელმისაწვდომია მხოლოდ კლიენტისთვის.** |
| არ ჩაითვლება. აღნიშნული ინფორმაცია არ არის მხოლოდ მომხმარებლისთვის ცნობილი და მათზე ხელი მიუწვდება სხვა პირებსაც.  ამასთან, ბარათზე ფიზიკურად დატანილი მონაცემების მსგავსად, მარტივია სხვა პირების მიერ მონაცემებზე წვდომდა. |

|  |
| --- |
| 1. **შეიძლება თუ არა, რომ პირადობის მოწმობის სპეციალური პროგრამული უზრუნველყოფით დასკანერება ჩაითვალოს ფლობის კომპონენტად? აღნიშნული პროგრამა ახდენს არამარტო პირადობაზე დატანილი ინფორმაციის წაკითხვას, არამედ ითვალისწინებს პირადობაზე დატანილ უსაფრთხოების კომპონენტებსაც.** |
| ფიზიკურად დატანილი ინფორმაციის ამოკითხვა არ მიიჩნევა ელემენტად.  ელექტრონული მონაცემების წაკითხვა უნდა განხორციელდეს სპეციალური წამკითხველებეის საშუალებით, ამ შემთხვევაში ეს მონაცემები შესაძლოა განხილულ იქნას ფლობის ელემენტად. |

|  |
| --- |
| 1. **შესაძლებელია თუ არა კლიენტის მიერ შესრულებული ბოლო ტრანზაქციების ცნობა ჩაითვალოს ცოდნის კომპონენტად?** |
| დიახ, თუმცა არ უნდა შემოიფარგლოს მხოლოდ ბოლო ოპერაციის შესახებ კითხვით. უნდა არსებობდეს ბევრი კითხვა და ისინი უნდა იყოს კომბინაციაში. ასევე, წინასწარ არავისთვის უნდა იყოს ცნობილი თუ რომელი კითხვა იქნება მომხმარებლისთვის დასმული (რომელი კითხვა ‘შეირჩევა’ სისტემის მიერ). |

|  |
| --- |
| 1. **მომხმარებლის მიერ ანგარიშზე წვდომისას („შესვლისას“), სანდო მოწყობილობიდან პასკოდით/ თითის ანაბეჭდით/ სახის ამომცნობით შესვლა ჩაითვლება თუ არა ძლიერ ავთენტიფიკაციად?** |
| ფლობის კატეგორიის ელემენტს წარმოადგენს აპლიკაცია, რომელიც **დაკავშირებულია** კონკრეტულ მოწყობილობასთან. სხვა კატეგორიის მეორე ელემენტად შესაძლებელია გამოყენებული იქნეს როგორც პასკოდი (ცოდნის კატეგორიის ელემენტი), ასევე, თითის ანაბეჭდი ან სახის ამომცნობი (უნიკალურობის კატეგორიის ელემენტები).  ზემოხსენებული კომბინაციის გამოყენება, კერძოდ აპლიკაციისა და პასკოდიის ერთობლიობა, წესთან შესაბამისია, თუ პასკოდში გულისხმობთ პაროლს. ხოლო, თუ მასში მოიაზრებთ ერთჯერად კოდს (ე.წ. OTP), აღნიშნული კომბინაცია ვერ დააკმაყოფილებს წესის მოთხოვნებს, რადგან კატეგორია გამეორდება (ორივე ფლობის კატეგორიის ელემენტია). წესის თანახმად, გამოყენებული უნდა იქნეს სულ მცირე ორი ელემენტი განსხვავებული კატეგორიებიდან. |

|  |
| --- |
| 1. **შეიძლება თუ არა 1 სანდო მოწყობილობა ქონდეს რამდენიმე ადამიანს?** |
| წესი არ განსაზღვრავს სანდო მოწყობილობის ცნებას და ასევე არ მოიცავს ჩანაწერს ერთი მოწყობილობის ერთზე მეტი ადამიანის მიერ გამოყენების შესახებ.  თუ ერთი მოწყობილობის გამოყენება განხორციელდება რამდენიმე მომხმარებლის მიერ, როგორც ფლობის კატეგორია, თანმდევი რისკები შესაბამისად უნდა იქნას შეფასებული. |

|  |
| --- |
| 1. **რა შეიძლება იგულისხმებოდეს ფლობის კატეგორიის რეპლიკაციაში და როგორ უნდა ავიცილოთ თავიდან რეპლიკაცია.** |
| მოწყობილობის იდენტიფიცირება შეიძლება მისი მოდელის, სხვა ინფორმაციის (მაგალითად, IMEI), სიმ ბარათის იდენთიფიკატორების და სხვა ინფორმაციის საშუალებით. თუმცა, თქვენი კითხვიდან გამომდინარე, თაღლითმა შესაძლოა აღნიშნული მონაცემების გამოყენებით შექმნას იდენტური ვირტუალური გარემო და აპლიკაციამ სხვა მოწყობილობა აღიქვას პროვაიდერის მომხმარებლის მოწყობილობად.  აღნიშნულის გამოსარიცხად, როდესაც პროვაიდერი ახორციელებს აპლიკაციის მოწყობილობასთან დაკავშირებას, შესაძლებელია აპლიკაცია იმგვარად იყოს მოწყობილი, რომ ზემოხსენებული ინფორმაცია მოწყობილობის შესახებ აქციოს დაშიფრულ ინფორმაციად და სწორედ მისი საშუალებით მოახდინოს აპლიკაციის დაკავშირება. შესაბამისად, სხვა პირმა რომ მოიპოვოს მოწყობილობის შესახებ ინფორმაცია, დაშიფრულ ინფორმაციას არ დაემთხვევა.  გთხოვთ, იხილოთ ამნარიდი EBA-ს მოსაზრებების დოკუმენტიდან (<https://bit.ly/2Jf2urq>):  “26. The EBA is of the view that approaches relying on mobile apps, web browsers or the exchange of (public and private) keys may also be evidence of possession, provided that they include a device binding process that ensures a unique connection between the PSU’s app, browser or key and the device. This may, for instance, be through hardware crypto-security, web-browser and mobile-device registration or keys stored in the secure element of a device. By contrast, an app or web browser that does not ensure a unique connection with a device would not be a compliant possession element.”. |

|  |
| --- |
| 1. **წესთან შესაბამისია შემდეგი პროცესი?**   **მომხმარებელი ახორციელებს თავის ანგარიშზე შესვლას სახელით და პაროლით, ადასტურებთ შესვლას OTP კოდით, რომელიც მისდის ან სმს ან ელ ფოსტზე. ამის შემდეგ მომხმარებლის გარემო, ტელეფონი ან კომპიუტერი ან ნებისმიერი ის მოწყობილობა რომლითაც მოახდინა შესვლა ხდება აპლიკაციასთან დაკავშირებული.** |
| ანგარიშზე წვდომა ძლიერი ავთენთიფიკაციის საფუძველზე ავტომატურად არ გულისხმობს აპლიკაციისა და მოწყობილობის დაკავშირებას/ბმას.  განსაკუთრებული ყურადღება უნდა მიექცეს ისეთ მოწყობილობასთან დაკავშირებას, რომლის გამოყენება მომხმარებლის მიერ პირველად ხდება. პროვაიდერმა უნდა გაატაროს დამატებითი ქმედებები იმის დასადასტურებლად, რომ უშუალოდ უფლებამოსილი მომხმარებლის მიერ ხდება მოწყობილობის გამოყენება აპლიკაციის გასააქტიურებლად. |

|  |
| --- |
| 1. **პროვაიდერის ელექტრონულ საფულეზე წვდომისთვის, მომხმარებელი ექვემდებარება შემდეგ ბიჯებს - Username, Password და OTP დაფიქსირებას ელ. საფულის პორტალზე. ელ. საფულეზე წვდომისას მომხმარებლის მიერ Password (ცოდნის ელემენტი) და OTP-ს (ფლობის ელემენტი) გამოყენებით შეხრულებული ძლიერი ავთენტიფიკაცია შეესაბამება წესის მოთხოვნებს?** |
| დიახ. აღწერილი ელემენტების ჭრილში შეესაბამება წესის მოთხოვნებს. ამ ელემენტების საფუძველზე უნდა გენერირდებოდეს ავტენთიფიკაციის კოდი. |

|  |
| --- |
| 1. **სავალდებულოა ძლიერი ავთენტიფიკაცია, მხოლოდ საგადახდო ანგარიშზე წვდომის (ხედვის) მიზნებისთვის? მომხმარებელს უნდა ჰქონდეს შესაძლებლობა თავად აირჩიოს ძლიერი ავთენტიფიკაციით განხორციელდეს ანგარიშზე წვდომა თუ არა?** |
| წესის მე-12 მუხლი ადგენს გამონაკლისს, როდესაც პროვაიდერი უფლებამოსილია მომხმარებელს შესთავაზოს ანგარიშზე წვდომა „ხედვის რეჟიმში“ ძლიერი ავთენტიფიკაციის გარეშე. სხვა შემთხვევებში, მომხმარებლის მიერ ანგარიშზე წვდომა უნდა განხორციელდეს ძლიერი ავთენტიფიკაციის საფუძველზე. ამ უკანსაკნელ შემთხვევაში, მომხმარებელს არ უნდა ჰქონდეს არჩევანის გაკეთების შესაძლებლობა. |

|  |
| --- |
| 1. **მე-3 მუხლის პუნქტი 1-ის მიხედვით ძლიერი ავთენტიფიკაცია საჭიროა დისტანციურად ონლაინ რეჟიმში თავის საგადახდო ანგარიშზე წვდომისთვის, რაც 6.1 პუნქტთან ერთად ნიშნავს იმას, რომ კლიენტი მობილურ ბანკში რომ log-in-ს აკეთებს თითის ანაბეჭდთან ერთად პაროლიც უნდა გამოიყენოს?** |
| დიახ, თითის ანაბეჭდისა და პინის ერთობლივად გამოყენება არის ძლიერი ავთენტიფიკაცია. ასევე, შესაძლებელი სხვა კატეგორიების კომბინაციის გამოყენებაც.  წესში მოცემულია გამონაკლისით სარგებლობის შემთხვევები. შესაბამისად შესაძლებელია ძლიერი ავთენტიფიკაცია არ განხორციელდეს განსაზღვრულ შემთხვევებში. |

|  |
| --- |
| 1. **ონლაინ ბანკში შესვლის შემდეგ ძლიერი ავთენტიფიკაციის საფუძველზე, თითოეულ ოპერაციაზე ცალ-ცალკე უნდა მოხდეს ავთენტიფიკაციის განხორციელება (მაგ. OTP გენერირება)?** |
| დიახ, გადახდის ოპერაციის ინიციირებისას უნდა განხორციელდეს ძლიერი ავთენტიფიკაცია, თუ ოპერაციე რომელიმე გამონაკლისში არ ექცევა.  Furthermore, it is necessary to specify the requirements of the strong customer authentication that should be applied each time a payer accesses its payment account online, initiates an electronic payment transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuse, by requiring the generation of an authentication code which should be resistant against the risk of being forged in its entirety or by disclosure of any of the elements upon which the code was generated.  Regulation on SCA, recital 1,  <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.069.01.0023.01.ENG&toc=OJ:L:2018:069:TOC> |

|  |
| --- |
| 1. **მე-3 მუხლის მე-6 პუნქტის თანახმად შესაძლებელია ცოდნის კატეგორიის ელემენტის მეორედ გამოყენება. აღნიშნული ეხება მხოლოდ ოპერაციის ინიციირებას, თუ შესაძლებელია სხვა ქმედებებიც ვიგულისხმოთ?**   **შესაძლებელია თუ არა სხვა კატეგორიის დამახსოვრებული ელემენტის ხელმეორედ გამოყენება?** |
| ერთი სესიის ფარგლებში, გამოყენებული ცოდნის კატეგორიის ელემენტის ხელმეორედ გამოყენება ძლიერი ავთენთიფიკაციისთვის შესაძლებელია გადახდის ოპერაციის ინიცირების გარდა სხვა ქმედებებისთვისაც.  სხვა კატეგორიის დამახსოვრებული ელემენტის ხელმეორედ გამოყენება წესით არ არის დაშვებული. |

|  |
| --- |
| 1. **ბარათის მონაცემებს + OTP კომბინაციით ინტერნეტ/მობაილ ბანკის მონაცემების აღდგენა ყველაზე გავრცელებული მეთოდია დღეს. შესაძლებელია აღნიშნული მეთოდი შევინარჩუნოთ?** |
| გარდამავალი დებულებების მიხედვით ელექტრონული კომერციის ოპერაციების განხორციელება შესაძლებელია ბარათის მონაცემებისა და ერთჯერადი კოდის გამოყენებით 2022 წლის 1 იანვრამდე, თუმცა აღნიშნული ოპერაციებისთვის პროვაიდერების მხრიდან დადგენილია გარკვეული ლიმიტები, ასევე ოპერაციების შინაარსი შეზღუდულია.  ინტერნეტ-ბანკის შემთხვევაში იგივე მოდელით პაროლის შეცვლა უფრო დიდი რისკების მატარებელია, ვიდერე ელექტრონული კომერციის ოპერაციები, აქედან გამომდინარე პროვაიდერმა უნდა დანერგოს მომხმარებლის დამატებითი გადამოწმების მექანიზმები. |

|  |
| --- |
| 1. **Digital Onboarding-ის პროცესის თანმდევი პროცესია მომხმარებლის პირველადი ავტორიზაცია დისტანციურ არხში. შეგვიძლია თუ არა, რომ ონბორდინგის დროს, მომხმარებლის სათანადო იდენტიფიკაციის შემდგომ, მოვთხოვოთ კლიენტს მოწყობილობისთვის სანდოს სტატუსის მინიჭება და პირველადი ავტორიზაციისას ეს მოწყობილობა გამოყენებული იყოს როგორც ფლობის ელემენტი?** |
| შესაძლებელია, თუ ინფორმაციას სანდო მოწყობილობის შესახებ ბანკი წინასწარ ფლობს (ვიდრე ანგარიშზე წვდომა განხორციელდება). ბანკს უნდა ჰქონდეს ისეთი პროცედურები, რითაც ექნება მაქსიმალური რწუნება, რომ მოწყობილობა ეკუთვნის მომხმარებელს. |

|  |
| --- |
| 1. **საგადახდო ბარათი და მოწყობილობაზე მიბმული აპლიკაცია ითვლება თუ არა ფლობის ელემენტად?** |
| 1. საგადახდო ბარათი, რომელიც ავთენტიფიკაციის კოდის დინამიურობას უზრუნველყოფს და რომლის მონაცემების წაკითხვა ხდება სპეციალური წამკითხველების საშუალებით ითვლება ფლობის კატეგორიის ელემენტად. 2. აპლიკაცია, რომელიც დაკავშირებულია მოწყობილობასთან ითვლება ფლობის კატეგორიის ელემენტებად.   გთხოვთ, იხილოთ EBA-ს მოსაზრებების დოკუმენტი ელემენტებთან დაკავშირებით (<https://bit.ly/2Jf2urq>), სადაც განხილულია სხვადასხვა გადაწყვეტა და ელემენტ(ებ)ად მიჩნევის საკითხი. |

|  |
| --- |
| 1. **შესაძლებელია თუ არა რომ ჩაითვალოს ფლობა + ცოდნის ელემენტად შემდეგი:**   **ა) კლიენტი აგენერირებს OTP კოდს დიჯიპასის მოწყობილობაზე ან დიჯიპასის აპლიკაციაში;**  **ბ) ამისათვის შეჰყავს პინ კოდი მოწყობილობაში (იცის პინ კოდი, რომლის გარეშეც მოწყობილობა არ დააგენერირებს OTP კოდს).** |
| OTP კოდი წარმოადგენს ფლობის კატეგორიას, ხოლო კონკრეტულ ამ შემთხვევაში „პინ“-ი ვერ იქნება ცოდნის კატეგორიის ელემენტი, ვინაიდან პინ კოდის გამოყენება ხდება დიჯიპასისთვის. ასევე, გასათვალისწინებელია, რომ ავთენტიფიკაციის ორი ელემენტის საფუძველზე უნდა დაგენერირდეს ავთენტიფიკაციის კოდი. |

|  |
| --- |
| 1. **ბანკომატიდან თანხის განაღდებისთვის საკმარისია თუ არა ჩიპიანი/უკონტაქტო ბარათი და სტაციონალური პინი?**   **პოსზე/ემპოსზე/ტელეფონზე გადახდისას საკმარისია თუ არა ჩიპიანი/უკონტაქტო ბარათი და სტაციონალური პინი?** |
| დიახ, საკმარისია. აქვე, გასათვალისწინებელია, რომ ჩიპიანი ბარათების მხოლოდ DDA და CDA კატეგორია აკმაყოფილებს წესის მოთხოვნებს. |

|  |
| --- |
| 1. **ერთჯერად კოდში 3D კოდი იგულისხმება? 3D Secure v1.0 ვერსია საკმარისი იქნება თუ არა ამ მოთხოვნის დასაკმაყოფილებლად?** |
| „3D Secure v1.0“ ვერ უზრუნველყოფს წესის მოთხონების სრულად დაკმაყოფილებას. |

|  |
| --- |
| 1. **ელექტრონული გადახდისას ძლიერი ავთენტიფიკაციისთვის საკმარისია თუ არა ბარათის მონაცემები, CVV/CVC და SMS კოდი?** |
| ბარათზე ფიზიკურად დატანილი სტატიკური მონაცემები არ წარმოადგენს ავთენტიფიკაციის ელემენტს. შესაბამისად, ბარათზე არსებული CVV/CVC უნდა იყოს ცვალებადი, რათა ჩაითვალოს ფლობის ელემენტად. მოკლე ტექსტური შეტყობინებით ერთჯერადი კოდის მიღებაც მიიჩნევა ფლობის ელემენტად. ვინაიდან ორივე ფლობის კატეგორიის ელემენტია, მათი ერთობლიობა ვერ დააკმაყოფილებს წესის მოთხოვნას. ძლიერი ავთენტიფიკაციისთვის გამოყენებული სულ მცირე ორი ელემენტი უნდა იყოს სხვადასხვა კატეგორიიდან. |

|  |
| --- |
| 1. **რომელ კატეგორიად ითვლება ჩიპიანი ბარათი და დინამიური CVV/CVC კოდი?** |
| ელექტრონული კომერციის ოპერაციის დროს ჩიპიანი ბარათი, რომელიც დასტურდება დინამიური CVV/CVC კოდით, წარმოადგენს ფლობის კატეგორიის ელემენტს. |

|  |
| --- |
| 1. **არსებობს ციფრული ბარათი, რომლის შესახებ ინფორმაციის მისაღებად ციფრულ არხში ავტორიზაცია (ანგარიშზე წვდომა) არის საჭირო. ჩაითვლება თუ არა ასეთი ბარათის მონაცემები (მაგ: CVV) ცოდნის კომპონენტად?** |
| იმ დაშვებით, რომ CVV მხოლოდ მომხმარებლისთვისაა ხელმისაწვდომი ინტერნეტ/მობაილ-ბანკში (ე.ი. მიუწვდომელია ბანკის თანამშრომლისთვის, საპროცესინგო ცენტრისთვის და ა.შ.) და ის ამავდროულად ცვალებადი არ არის, ჩაითვლება ცოდნის კატეგორიის ელემენტად. ამასთან, ცოდნის კატეგორიის მიმართ დაცული უნდა იყოს წესის მე-8 მუხლის მოთხოვნები. მაგალითისთვის, ცოდნის კატეგორიას მიეკუთვნება PIN-ი. რეკომენდებულია უზრუნველყოფილი იქნეს ციფრული ბარათის CVV-ის ისეთივე დაცვა, როგორც ეს ხდება PIN-ის შემთხვევაშია.  კითხვაში სრულად არ არის ასახული თუ რა ოპერაციაზეა საუბარი. აქედან გამომდინარე, სრულყოფილი პასუხის გასაცემად მნიშვნელოვანია ასევე სხვა ელემენტის დადგენაც. |

|  |
| --- |
| 1. **ბანკომატის ინტერფეისში ძლიერი ავთენთიფიკაციის საფუძველზე შესვლის შემდეგ, თანხის გასანაღდებლად ისევ საჭიროა ძლიერი ავთენტიფიკაცია?** |
| ბანკომატის ინტერფეისში ძლიერი ავთენთიფიკაციის საფუძველზე შესვლის შემდეგ, დამატებითი ძლიერი ავთენთიფიკაციის გარეშე შესაძლებელია მხოლოდ ერთი ოპერაციის შესრულება. |

|  |
| --- |
| 1. **პინ-ის ცვლილება შესაძლებელია ბანკომატიდან. საჭიროა თუ არა დამატებითი ავთენტიფიკაცია?** |
| თუ მომხმარებელი ბანკომატთან იყენებს ბარათსა და პინ კოდს, რათა ინტერფეისზე წვდომა იქონიოს, ამის შემდგომ მხოლოდ პინ კოდის შეცვლისთვის დამატებითი ძლიერი ავთენტიფიკაციის განხორციელება სავალდებულო არ არის. |

|  |
| --- |
| 1. **ელ. კომერციის „ჩექაუთის“ ერთ-ერთი ვარიანტის დროს, კლიენტი გადის ორფაქტორიან ავტორიზაციას ინტერნეტ ბანკის იუზერით და პაროლით. შემდეგ კლიენტს უჩანს მისი ბარათების სია, ირჩევს ერთ-ერთ ბარათს და იხდის. კლიენტი ავთენტიფიკაციას გადის და სესია იქმნება მხოლოდ ერთი გადახდისათვის. ასევე, თუ მომხმარებელს ბარათის არჩევის დროს გამოუჩნდება ბარათებზე არსებული ნაშთები, ბარათის არჩევის შემდეგ კიდევ ერთხელ მოუწევს ავთენტიფიკაცია?** |
| თუ აღწერილი პროცესის მიზანია მხოლოდ იმ ერთი ოპერაციის შესრულება და შეუძლებელი იქნება სხვა ოპერაციის ინიციირება, პროცესი არ ეწინააღმდეგება წესს. იქედან გამომდინარე, რომ ანგარიშზე არსებული ნაშთის ნახვა წესის გამონაკლისის შესაბამისად შესაძლებელია ძლიერი ავთენტიფიკაციის გარეშე, ხსენებულ შემთხვევაშიც დასაშვებია.  ამ პროცესში ასევე გასათვალისწინებელია ავთენტიფიკაციის კოდის გენერირების მოთხოვნები. |

|  |
| --- |
| 1. **„NFC“ საფულის შემთხვევაში, ხდება აპლიკაციაში შესვლა (ძლიერი ავტენთიფიკაცია) და შემდეგ გადახდისას არაფერს ვთხოვთ მომხმარებელს. შეესაბამება თუ არა წესს?** |
| აპლიკაციაში შესვლის შემდეგ, გადახდისას დაცული უნდა იყოს უკონტაქტო გადახდების (მე-13 მუხლი) მიმართ დადგენილი მოთხოვნები. |

|  |
| --- |
| 1. **თუ სავაჭრო ობიექტი არ არის 3d enrolled, რა მექანიზმები რჩება ძლიერი ავთენტიფიკაციისთვის?** |
| თუ გადახდა ბარათით ხდება, მაშინ საბარათე სქემამ და მისმა მონაწილეებმა უნდა უზრუნველყონ ტექნიკურ დონეზე ძლიერი ავთენტიფიკაციის მხარდაჭერა.  ასევე გთხოვთ იხილოთ დამატებითი ინფორმაცია (გვერდი 20. პუნქტი 7.3-დან)  7.3 [cards] For card transactions, all card issuing PSPs should support strong authentication of the cardholder. All cards issued must be technically ready (registered) to be used with strong authentication.  7.4 [cards] PSPs offering acquiring services should support technologies allowing the issuer to perform strong authentication of the cardholder for the card payment schemes in which the acquirer participates.  7.5 [cards] PSPs offering acquiring services should require their e-merchant to support solutions allowing the issuer to perform strong authentication of the cardholder for card transactions via the internet. The use of alternative authentication measures could be considered for preidentified categories of low-risk transactions, e.g. based on a transaction risk analysis, or involving low-value payments, as referred to in the Payment Services Directive.  7.6 All payment schemes should promote the implementation of strong customer authentication by introducing a liability regime22 for the participating PSPs in and across all European markets.  7.7 [cards] For the card payment schemes accepted by the service, providers of wallet solutions should require strong authentication by the issuer when the legitimate holder first registers the card data.  7.8 Providers of wallet solutions should support strong customer authentication when customers log in to the wallet payment services or carry out card transactions via the internet. The use of alternative authentication measures could be considered for pre-identified categories of low-risk transactions, e.g. based on a transaction risk analysis, or involving low-value payments, as referred to in the Payment Services Directive.  <https://eba.europa.eu/documents/10180/855014/EBA-CP-2014-31+%28CP+on+security+of+internet+payments%29.pdf> |

|  |
| --- |
| 1. **რომელი მონაცემები მიეკუთვნება სენსიტიურ საგადახდო მონაცემებს?**   *ასევე, რატომ არის მხოლოდ თაღლითურ ოპერაციაზე ხაზგასმა, თუ სენსიტიური საგადახდო მონაცემებით ჩვეულებრივი, არათაღლითური ოპერაციის განხორციელებაც არის შესაძლებელი?* |
| „სენსიტიური საგადახდო მონაცემების“ განმარტების მიზანია, ისეთი მონაცემების იდენტიფიცირება, რომლის თაღლითის მიერ მოპოვების შემთხვევაში, თაღლითის მიერ შესაძლებელია ოპერაციის შესრულება.  აღნიშნულიდან გამომდინარე, ტერმინის განმარტებაში ხდება თაღლითობაზე ხაზგასმა. |

|  |
| --- |
| 1. **სხვადასხვა სტანდარტი სენსიტიურ მონაცემებს განმარტავს სხვადასხვაგვარად. გთხოვთ, დაგვიზუსტოთ კონკრეტული სენსიტიური საგადახდო მონაცემების ჩამონათვალი.** |
| წესი სენსიტიურ საგადახდო მონაცემს განმარტავს ამავე წესის მიზნებისთვის. შეუძლებელია ამ ტერმინში ამომწურავი ჩამონათალის განსაზღვრა იქედან გამომდინარე, რომ შესაძლოა მონაცემი ერთი პროვაიდერისთვის არ იყოს სენსიტიური, მეორისთვის კი ასეთს წარმოადგენდეს. აღნიშნული დამოკიდებულია იმაზე, შესაძლებელია თუ არა მონაცემის საშუალებით თაღლითური ოპერაციის განხორციელება. პრაქტიკაში გამოყენებული ყველა მონაცემების სენსიტიურად ჩათვლა დამატებით ტვირთს შექმნის ცალკეული პროვაიდერისთვის, რომელიც გადახდის ოპერაციის განხორციელებისთვის არ იყენებს ასეთ მონაცემს. |

|  |
| --- |
| 1. **თაღლითური ოპერაციის შესრულება შესაძლებელია ბარათის ვადის და ნომრის საფუძველზე, წარმოადგენს თუ არა ისინი სენსიტიურ საგადახდო მონაცემი?** |
| წესის შესაბამისად, ბარათზე ფიზიკურად დატანილი ინფორმაცია არ წარმოადგენს ძლიერი ავთენტიფიკაციის ელემენტებს. შესაბამისად, წესიდან გამომდინარე მხოლოდ ბარათზე დაბეჭდილი მონაცემებით საბარათე ოპერაცია არ უნდა განხორციელდეს, გარდა წესით გათვალისწინებული დაბალრისკიანი ოპერაციებისა.  თუ ინფორმაცია ფიზიკურად არ არის დატანილი, მაგრამ მხოლოდ ბარათის მფლობელმა იცის ან/და არსებობს ელექტრონული სახით (მაგ. ვირტუალური ბარათი), ის წარმოადგენს სენსიტიურ საგადახდო მონაცემს. |

|  |
| --- |
| 1. **წესი ამბობს, რომ კოდი საგადახდო მომსახურების პროვაიდერის მიერ ავთენტიფიკაციისთვის შეიძლება მიღებული იქნეს მხოლოდ ერთხელ.**   **პინ კოდი მრავალჯერადი გამოყენებისაა და, შესაბამისად, რას ნიშნავს ეს ჩანაწერი საბარათე ოპერაციებისთვის, კერძოდ პოს ტერმინალში და ბანკომატში გადახდისას პინის გამოყენებისთვის?** |
| აღნიშნული ჩანაწერი ეხება **ავთენტიფიკაციის კოდს.** ხოლო პინ კოდი არის ელემენტი, რომლის მეორე ელემენტთან ერთობლიობაში გენერირდება ავთენტიფიკაციის კოდი. |

|  |
| --- |
| 1. **საგადახდო ოპერაციის შესრულების დროს, დაგენერირებული ავთენტიფიკაციის კოდი დონამიურად დაკაშირებული უნდა იყოს ტრანზაქციის მიმღებთან და თანხასთან, ეს მოთხოვნა ეხება ერთჯერად კოდს (დიჯიპასის ან SMS ერთჯერადი კოდი)?** |
| დიჯიპასის ან SMS ერთჯერადი კოდი არის ავთენთიფიკაციის **ელემენტები.**  **ავთენტიფიკაციის კოდი** გენერირდება ავთენტიფიკაციის ორი ელემენტის საფუძველზე, რომელიც დინამიურად დაკავშირებული უნდა იყოს მიმღებთან და თანხასთან. |

|  |
| --- |
| 1. **მუხლი 6.2. - ავთენტიფიკაციის კოდის ერთჯერადობა.**   რიგ შემთხვევებში (ბანკომატის ან თვითმოსახურების კიოსკის გამოყენების დროს) იდენტიფიკაციისთვის ვიყენებთ საგადახდო ბარათს და შესაბამისი პინ კოდის კომბინაციას, მაგრამ ამ შემთხვევაში კოდი ვერ იქნება ერჯერადი გამოყენების. ამ პუნქტთან წინააღმდეგობაში მოდის აღწერილი პროცესი? |
| აღწერილი პროცესი არის ძლიერი ავთენთიფიკაცია, თუ ბარათის მონაცემების წაკითხვა ბარათიდან ხდება სპეციალური წამკითხველის საშუალებით (Card evidenced by a card reader), მაშინ ის ფლობის კატეგორიის ელემენტია, ხოლო პინი არის ცოდნის ელემენტი.  პინი **არ არის** ავთენთიფიკაციის კოდი. ავთენტიფიკაციის კოდი უნდა დაგენერირდეს ავთენტიფიკაციის ორი ელემენტის საფუძველზე. |

|  |
| --- |
| 1. **ძლიერი ავთენტიფიკაციის აუთსორსინგი შესაძლებელია?** |
| დიახ, შესაძლებელია. თუმცა, პროვაიდერი რჩება აღნიშნულ პროცესზე და მისგან გამოწვეულ შედეგებზე მომხმარებელთან სრულად პასუხისმგებელი. |

|  |
| --- |
| 1. **გრძელდება თუ არა იგივე სესია, თუ მომხმარებელს 5 წუთის შუალედში უფიქსირდება 1 აქტივობა მაინც.** |
| დიახ, გრძელდება, თუ მანამდე სხვა მიზეზით არ არის შეწყვეტილი. |

|  |
| --- |
| 1. **ნებისმიერ პერიოდში უმოქმედობის მაქსიმალური ხანგრძლივობა უწყვეტად არ უნდა აღემატებოდეს 5 წუთს. შესძლებელია თუ არა, 5 წუთთან მიახლოებულ დროს მომხმარებელს გამოუჩნდეს ღილაკი, მაგალითად, „სესიის გაგრძელება“, რომელზე დაჭერაც ჩაითვლება აქტიურობად და 5 წუთის ათვლა თავიდან დაიწყება?** |
| დიახ, შესაძლებელია. |

|  |
| --- |
| 1. **სწორია თუ არა, რომ 1 სესიის ფარგლებში SCA-ის გავლა მომხმარებელს განმეორებით აღარ მოეთხოვება?** |
| თუ პროვაიდერმა განახორციელა მომხმარებლის ძლიერი ავთენტიფიკაცია ანგარიშზე წვდომისთვის („log in“), აღნიშნულის შემდეგ იმავე სესიაში ქმედების განხორცილებისას, სავალდებულოა SCA-ს კვლავ განხორციელება (გამონაკლისების გარდა ყველგან). აღნიშნულის დროს დასაშვებია მომხმარებლის მიერ გამოყენებული ცოდნის კატეგორიის ელემენტის პროვაიდერის მიერ ხელახლა გამოყენება (reuse). ასეთ შემთხვევაში, მომხმარებელს უადვილდება პროცესი, რადგან თავად არ უწევს ცოდნის ელემენტის შეყვანა და ამატებს მხოლოდ ერთ ელემენტს (ფლობა (მაგ. OTP), ბიომეტრია). აღნიშნული გათვალისწინებულია წესის მე-3 მუხლის მე-5 პუნქტში. |

|  |
| --- |
| 1. **ავთენტიფიკაციის კოდი აუცილებლად უნდა მონაწილეობდეს თუ არა გადახდის დადასტურების პროცესში. ანუ ავთენტიფიკაციის გავლის შემდეგ მომხმარებელს უნდა ვაჩვენოთ კოდი რომელიც უნდა შეიყვანოს გადახდის დასადასტურებლად?** |
| ავთენტიფიკაციის კოდი გენერირდება მომხმარებლის მიერ შეყვანილი ელემენტების საფუძველზე. უშუალოდ ავთენტიფიკაციის კოდის შეყვანა მომხმარებლის მიერ არ ხორციელდება. |

|  |
| --- |
| 1. **მუხლი 5.4.ა. - მომხმარებელი ვერ უნდა მიხვდეს უარის მიზეზს?**   „ა) თუ ... კოდის გენერირება წარუმატებელი აღმოჩნდა, შედეგად შეუძლებელი უნდა იყოს გამოყენებული ელემენტებიდან მცდარი ელემენტის (ელემენტების) იდენტიფიცირება;“ |
| მომხმარებელს მიეწოდება ინფორმაცია, რომ ელემენტების შეყვანისას მოხდა შეცდომა, თუმცა დაუშვებელია კონკრეტულ ელემენტზე მითითება, გარდა წესით გათვალისწინებული შემთხვევებისა. |

|  |
| --- |
| 1. **წესის შესაბამისად, შეუძლებელი უნდა იყოს გამოყენებული ელემენტებიდან მცდარი ელემენტის/ელემენტების იდენტიფიცირება. ბიომეტრიული მონაცემებით ავთენტიფიკაციის შემთხვევაში, წარუმატებელი ავთენტიფიკაციის შესახებ შეტყობინება შესაძლოა დამოკიდებული იყოს მობილური მოწყობილობის პროგრამულ უზრუნველყოფაზე - მან შეატყობინოს მომხმარებელს, რომ თითის ანაბეჭდი არ დაემთხვა. შესაბამისად ამ პარამეტრს ბანკი ვერ გააკონტროლებს.** |
| წესი ზღუდავს პროვაიდერის მიერ ინფორმაციის მიწოდებას. იმ შემთხვევაში, როდესაც პროვაიდერი ეყრდნობა მოწყობილობაში შენახულ ანაბეჭდთან დადარებას, პროვაიდერის აპლიკაციამ მომხმარებელს არ უნდა მიაწოდოს ინფორმაცია დამთხვევის წარუმატებლობის შესახებ. |

|  |
| --- |
| 1. **ავთენტიფიკაციის წარუმატებლობისას რა სახით უნდა მოხდეს ინფორმაციის მიწოდება, ისე რომ მცდარი ელემენტის იდეტიფიცირება შეუძლებელი იყოს? შესაძლებელია „დაფიქსირდა შეცდომა“, „სისტემური შეცდომა“ ან მსგავსი მისაღებია?** |
| მთავარია არ მოხდეს მცდარი ელემენტის იდენტიფიცირება და მომხმარებლისთვის ინფორმაციის მიწოდება. წესი არ განსაზღვრავს ინფორმაციის ფორმულირებას. |

|  |
| --- |
| 1. **კოდის გენერირების წარუმატებლობის შემთხვევაში შეუძლებელი უნდა იყოს გამოყენებული ელემენტებიდან მცდარი ელემენტის/ ელემენტების იდენტიფიცირება. ბარათის შემთხვევაში ეს მხოლოდ ელ. კომერციას ეხება თუ ფიზიკურ ტერმინალებში შერულებულ ოპერაციებსაც? რა მიდგომაა ბანკომატებთით თანხის განახდების მიმართ?** |
| აღნიშნული არ ეხება ფიზიკური პოს-ტერმინალის საშუალებით გადახდას და ბანკომატის საშუალებით განაღდებას. წესის მე-6 მუხლს დაემატა მე-8 პუნქტი, რომელიც განსაზღვრავს, რომ ხსენებული მოთხოვნა არ ვრცელდება საბარათე ინსტრუმენტის საშუალებით ფიზიკური პოს-ტერმინალისა და ბანკომატის საშუალებით გადახდის ოპერაციის ინიციირებისას. |

|  |
| --- |
| 1. **OTP-ს მიღების შემდეგ გადამხდელმა თუ შეცვალა მიმღები ან/და თანხა ამ OTP-მ არ უნდა იმუშაოს, თუ ავთენტიფიკაციის კოდმა?** |
| წესის ეს მოთხოვნა ეხება ავთენტიფიკაციის კოდს, თუმცა ეს მოთხოვნა არ კრძალავს OTP-ს კონკრეტული თანხისთვის და მიმღებისთვის გენერირების შესაძლებლობას. |

|  |
| --- |
| 1. **მომხმარებლისთვის მოკლე ტექსტური შეტყობინებით ერთჯერადი კოდის გაგზავნა უცხოეთში პრობლემატურია. მომხმარებელს უნდა შეეძლოს დინამიური კოდის გარეშე ოპერაციის დადასტურება.** |
| წესი არ განსაზღვრავს ერთჯერადი კოდის ერთ-ერთ ელემენტად გამოყენების და ყველა გადახდის თუ ქმედების მიმართ იმავე კომბინაციის გამოყენების ვალდებულებას. შესაძლებელია გამოყენებული იქნეს კონკრეტულ შემთხვევებზე მორგებული ელემენტების კომბინაციები. |

**აუდიტი და მონიტორინგის სისტემები**

|  |
| --- |
| 1. **ტრანზაქციის განხორციელება ხდება ონ-ლაინ რეჟიმში, აქ მოიაზრება ონ-ლაინ მონიტორინგიც?[[1]](#footnote-1)** |
| სიცხადისთვის მიზანშეწონილია, გაიმიჯნოს მონიტორინგის მიმართ წესის ორი მუხლის მოთხოვნები:   1. მუხლი 3 - **გადახდის ოპერაციის მონიტორინგის მექანიზმი**   ამ მუხლის მოთხოვნები ვრცელდება ყველა პროვაიდერზე. გადახდის ოპერაციის მონიტორინგის მექანიზმი უნდა არსებობდეს ძლიერი ავთენტიფიკაციის მექანიზმის პარალელურად. მონიტორინგი შესაძლოა განხორციელდეს ოპერაციის განხორციელების შემდგომ, თუმცა ვინაიდან პროვაიდერი ვალდებულია ჰქონდეს მონიტორინგის მექანიზმი, რეკომენდებულია, იმ გადახდებზეც, რომლებიც არ სრულდება მყისიერად, მონიტორინგი განხორციელდეს მათ შესრულებამდე. ზემოხსენებულ შემთხვევებში, არ არის სავალდებულო მისი განხორციელება დროის რეალურ რეჟიმში.  აქვე გასათვალისწინებელია წესის მოთხოვნა, რომლის მიხედვითაც, დავალების მყისიერი შესრულების შემთხვევაში, პროვაიდერი ვალდებულია განახორციელოს დროის რეალურ რეჟიმში მონიტორინგი.     1. მუხლი 20 - **გადახდის ოპერაციის რისკის ანალიზი**   „გადახდის ოპერაციის რისკის ანალიზის“ მოთხოვნა ვრცელდება მხოლოდ იმ პროვაიდერებზე, რომლებთაც სურთ ისარგებლონ მე-20 მუხლის პირველი პუნქტით დაშვებული გამონაკლისით (კერძოდ, არ გამოყენოთ მომხმარებლის ძლიერი ავთენთიფიკაციის მექანიზმი დაბალი რისკის ტრანზაქციებისთვის). აღნიშნულმა პროვაიდერებმა უნდა განახორციელონ ოპერაციის რისკის ანალიზი დროის რეალურ რეჟიმში (ოპერაციის დადასტურებამდე).  როგორც ზემოთ არის მითითებული, ასეთი მექნიზმი ასევე უნდა იქნეს გამოყენებული იმ შემთხვევაში, როდესაც ოპერაცია მყისიერად ხორციელდება.  <https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4090>  „Accordingly, for payments service providers to be able to benefit from the transaction risk analysis exemption under Article 18 of the RTS, they have to go beyond the general monitoring requirements required under Article 2 of these RTS and have mechanisms in place that enable “real time risk monitoring”, in other words a monitoring before the transaction is authorised. The general monitoring mechanism under Article 2 of these RTS does not require enabling ‘real time risk monitoring’ and is usually carried out “after” the execution of the payment transaction.“ |

|  |
| --- |
| 1. **გთხოვთ, დაგვიკონკრეტოთ რა იგულისხმება აღნიშნულ ჩანაწერში - ოპერაციის მყისიერად შესრულება. ყველა ოპერაცია სრულდება მყისიერად, შესაბამისად გთხოვთ, მოგვიყვანოთ მაგალითიც.** |
| მყისიერად შესრულება გულისხმობს დავალების მიღებისთანავე შესრულებას. აღნიშნულში შედის როგორც ე.წ. სწრაფი გადახდების სისტემით შესრულებული ოპერაციები (სხვადასხვა პროვაიდერების მომხმარებლებს შორის), ასევე ერთი პროვაიდერის სხვადასხვა მომხმარებლებს შორის შესრულებული ოპერაციები. |

|  |
| --- |
| 1. **პროვაიდერი ვალდებულია ჰქონდეს გადახდის ოპერაციების მონიტორინგის მექანიზმი, რომლითაც ის შეძლებს არაავტორიზებული ან/და თაღლითური გადახდის ოპერაციების იდენტიფიცირებას. აქ მხოლოდ დეტექცია (და შემდგომ მანუალური რეაგირება) საკმარისია თუ პროგრამულ გადაწყვეტილებას ასევე უნდა ქონდეს რეალურ რეჟიმში პრევენციის საშუალებაც?** |
| ეს წესი არ მოითხოვს დეტექციის საფუძველზე ავტომატიზირებულ რეაგირებას. პროვაიდერის მიერ გადასაწყვეტია მონიტორინგის სისტემით დაფიქსირებული ტრანზაქციებიდან რომელი დაბლოკოს ავტომატურ რეჟიმში და რომელი არა მომხმარებლის ინტერესების გათვალისწინებით. |

|  |
| --- |
| 1. **სტანდარტული რისკ-მონიტორიგნის სისტემა ვერ დაფარავს ამ საკითხს (3.3.), ამ შემთხვევაში ბანკს უნდა ქონდეს რეალიზებული მაგ 3DS 2?** |
| სებ-ი ტექნოლოგიური ნეიტრალიტეტის („technology- and business-model neutral“) გათვალისწინებით სავალდებულოდ არ განსაზღვრავს რაიმე ტექნოლოგიას ან სტანდარტს. თუმცა, საბარათე ოპერაციების ჭრილში EBA-ს მოსაზრების თანახმად, “3D secure version 2.2” უზრუნველყოფს SCA-სთან სრულ თავსებადობას. |

|  |
| --- |
| 1. **გულისხმობს თუ არა სპეციალური პროგრამული/აპარატურული უზრუნველყოფის შესყიდვის აუცილებლობას წესების მე-3 მუხლის მე-2 პუნქტში ნახსენები მონიტორინგის „მექანიზმი“-ს უზრუნველყოფა?** |
| დამოკიდებულია პროვაიდერის არსებულ ინფრასტრუქტურაზე/პროგრამულ უზრუნველყოფაზე. პროვაიდერის შესაფასებელია, რამდენად უზრუნველყოფს მისი არსებული სისტემა წესის მოთხოვნების შესარულებას.  პროვაიდერი თავისუფალია არჩევანში - შეიძინოს ან თავად განავითაროს პროგრამული უზრუნველყოფა. |

|  |
| --- |
| 1. **რა იგულისხმება წესში გამოყენებულ ტერმინში „კომპრომეტირება“?** |
| დარღევა, ხელყოფა, არაუფლებამოსილი მოპოვება/გამოყენება და სხვა. |

|  |
| --- |
| 1. **მუხლი 3.4.ა. - იგულისხმება, თუ არა, რომ პროვაიდერმა უნდა მოახდინოს იდენტიფიცირება/მონიტორინგი კონკრეტულად რომელი ელემენტების კომპრომეტირება მოხდა თაღლითობის დროს?** |
| აღნიშნული ქვეპუნქტის მიხედვით, პროვაიდერს უნდა გააჩნდეს კომპრომეტირებული/მოპარული ელემენტების სია და ამ სიას უნდა შეადაროს მომხმარებლის მიერ გამოყენებული ელემენტები. |

|  |
| --- |
| 1. **რომელ „თითოეულ ოპერაციას“ გულისხმობს მე-3 მუხლის 4.ბ. პუნქტის ჩანაწერი ? საეჭვო ან უჩვეულო ნიშნების ოპერაციას?** |
| წესის მე-3 მუხლის მე-4 პუნქტი:  „საგადახდო მომსახურების პროვაიდერი ვალდებულია უზრუნველყოს, რომ გადახდის ოპერაციების მონიტორინგის მექანიზმი ითვალისწინებდეს, სულ მცირე, რისკზე დაფუძნებულ შემდეგ ფაქტორებს: … ბ) თითოეული გადახდის ოპერაციის თანხას; ...“  მონიტორინგი ხორციელდება თითოეული ოპერაციის თანხის ოდენობის გათვალისწინებით. შესაძლოა თანხა დამოუკიდებლად არ იყოს საეჭვო/უჩვეულო, თუმცა სხვა ფაქტორებთან გათვალისწინებით იყოს. |

|  |
| --- |
| 1. **რა არის წყარო ამ თაღლითობის ცნობილი სცენარების მოძიებისთვის?** |
| აღნიშნულის მოძიება თავად პროვაიდერის პასუხისმგებლობაა.  საწყის ბაზად საერთაშორისო ფროდების ტიპოლოგია შეიძლება იყოს აღებული და დაემატოს ლოკალური ფროდების ტიპოლოგია. |

|  |
| --- |
| 1. **გვაქვს თუ არა ვალდებულება წინასწარ შევათანხმოთ მარეგულირებელთან მიდგომები, რომლის გამოყენებითაც მოხდება ოპერაციებზე მონიტორინგი?** |
| მონიტორინგის პროცესებს თავად პროვაიდერი განსაზღვრავს და არ საჭიროებს სებ-თან შეთანხმებას. |

|  |
| --- |
| 1. **მუხლი 3.4.ე. - გთხოვთ, განმარტოთ მოთხოვნები. უჩვეულო გამოყენება რა არის?** |
| პროვაიდერს უნდა ჰქონდეს მონიტორინგის მექანიზმი, რისი საშუალებითაც „შეისწავლის“ კონკრეტული პირის ქმედებებს, რომელიც მისთვისაა დამახასიათებელი. მოწყობილობისა და უზრუნველყოფის გამოყენების ადგილი, სიხშირე, პერიოდი, და ა.შ.  „უჩვეულო გამოყენება“ გულისხმობს ზემოაღნიშნულისგან განსხვავებულ ქმედებას. |

|  |
| --- |
| 1. **ავთენტიფიკაციის პროცესის თითოეულ სესიაში შეფერხების ან/და დაზიანების გამომწვევი, ასევე ინფორმაციაზე არაუფლებამოსილი წვდომისთვის განკუთვნილი ფარული პროგრამული უზრუნველყოფა რას გულისხმობს?** |
| დამკვიდრებული ტერმინოლოგიით აღნიშნული გულისხმობს, მაგალითად, ე.წ. malware-ს. |

|  |
| --- |
| 1. **როგორ უნდა გახორციელდეს მე-3 მუხლის მე-4 პუნქტის „დ“ ქვეპუნქტის შესრულება, სადაც მოთხოვნილია ავთენტიფიკაციის პროცესის თითოეულ სესიაში შეფერხების ან/და დაზიანების გამომწვევი, ასევე ინფორმაციაზე არაუფლებამოსილი წვდომისთვის განკუთვნილი ფარული პროგრამული უზრუნველყოფის არსებობის ნიშნების იდენტიფიცირება.** |
| წესი არ განსაზრვრავს თუ როგორ უნდა განხორციელდეს პროვაიდერის მიერ არნიშნული მოთხოვნის შესრულება, თუმცა მაგალითისთვის, შეგიძლიათ იხილოთ endpoint malware detection-ის შესახებ მცირე ინფორმაცია:  „For an endpoint malware detection control to succeed in the current environment, there are two key properties it must have. First, it must be invisible to attackers. Therefore it must reside in the kernel rather than in user space. If it resides in user space, it can be detected, attacked, and disabled by the adversary.  Second, it must be able to detect a rich range of malicious behavior. Some are calling these behaviors, “conditions” for a successful compromise.  An information technology example might be that malware must be able to write temporary files. However, good software might also need to write temporary files. On the other hand, it would be highly unlikely that a PDF needs to write a temporary file.  Therefore, a good endpoint malware detection control must be able to detect “conditions” of malware. However, just as noted above, a single indicator of malware is not enough to “convict” a piece of software. Once a condition/indicator is detected, that software in question must be watched carefully to determine if it’s really malware. The processing needed for this approach is significant, and if done on the endpoint, would surely degrade its performance. Therefore this type solution needs a console/server with significant compute power to monitor all of the endpoints exhibiting conditions/indicators of malware“.  **შენიშვნა:** ციტირება მხოლოდ მაგალითისთვის და ზოგადი ინფორმაციისთვის. ციტირება არ ემსახურება/არ წარმოადგენს სებ-ის მიერ რეკომენდაციას ან/და მითითებას ინფორმაციაზე ან მის განმათავსებელზე. ამასთან, წესის მოთხოვნის შესრულების შესაძლებლობას არ ავიწროვებს ციტირებულ ტექსტში მოყვანილ ინფორმაციამდე. <https://www.cymbel.com/zero-trust-recommendations/endpoint-malware-detection/> |

|  |
| --- |
| 1. **წესში მითითებულია, რომ პროვაიდერი ვალდებულია დაიცვას პროგრამის ან/და არხის უსაფრთხოება.**   **მნიშვნელოვანია დაკონკრეტდეს იმ მინიმალური ტექნოლოგიური უსაფრთხოების საშუალებების ჩამონათვალი, ასევე გაიმიჯნოს პროვაიდერისა და მისი მომხმარებლის პასუხისმგებლობები;** |
| ტექნიკური უსაფრთხოების საშუალებებს განსაზღვრავს თავად პროვაიდერი თავისი ბიზნეს მოდელიდან გამომდინარე. რაც შეეხება პასუხისმგებლობას, აღნიშნული წესის დაცვა პროვაიდერის ვალდებულებაა.  მომხმარებლის პასუხისმგებლობას განსაზღვრავს „საგადახდო სისტემისა და საგადახდო მომსახურების შესახებ“ კანონი. |

|  |
| --- |
| 1. **რა არის აუდიტის ჩატარების ფარგლები (მუხლი 5.1.)?** |
| „This audit shall present an evaluation and report on the compliance of the payment service provider's security measures with the requirements set out in this Regulation.“  აუდიტი სულ მცირე უნდა მოიცავდეს წესის მე-2 თავის მოთხოვნებთან შესაბამისობის ანგარიშს, ასევე მე-20 მუხლით დადგენილი გამონაკლისით სარგებლობის შემთხვევაში, შესაბამისი მეთოდოლოგიის, მოდელისა და ანგარიშგებით მიწოდებული (შეტყობინებული) თაღლითობის მაჩვენებლების აუდიტს. |

|  |
| --- |
| 1. **რა იგულისხმება უსაფრთხოების ზომების დოკუმენტირებაში?** |
| სავალდებულოა წესით განსაზღვრული უსაფრთხოების ზომების დანერგვის დოკუმენტირება. ე.ი. მათი როგორც თავდაპირველი მდგომარეობის, ასევე, ცვლილებების აღწერა. |

|  |
| --- |
| 1. **რა არის მინიმალური პერიოდული შემოწმების ვადები და უსაფრთხოების ზომების ჩამონათვალი?** |
| აუდიტის ჩატარების დროსთან მიმართებით გთხოვთ იხილოთ მე-5 მუხლი და 31-ე მუხლი.  უსაფრთხოების ზომების შესახებ ინფორმაცია მოცემულია წესის მე-2 თავში. |

|  |
| --- |
| 1. **დოკუმენტში მითითებულია, რომ საგადახდო მომსახურების პროვაიდერის აუდიტი უნდა განხორციელდეს კვალიფიციური აუდიტორის მიერ. მნიშვნელოვანია დაკონკრეტდეს, თუ რა კვალიფიკაციის მქონე პირს შეეძლება ჩაატაროს აუდიტი. ასევე ბუნდოვანია აუდიტის მიზანი, უნდა მოიცავდეს ეს მხოლოდ სისტემის შესაბამისობას აღნიშნულ წესთან თუ სხვა სახის, მაგალითად ფინანსურ აუდიტს.** |
| წესში განსაზღვრული აუდიტი მოიცავს მხოლოდ წესის მოთხოვნებთან შესაბამისობის ანგარიშს და არ მოიცავს ფინანსურ აუდიტს.  აუდიტორს უნდა შეეძლოს ტექნოლოგიური გადაწყვეტის დონეზე პროცესების შეფასება. |

|  |
| --- |
| 1. **კომერციული ბანკი, ვალდებულია თუ არა რეგისტრირებული საგადახდო მომსახურების პროვაიდერის შემოწმებაზე, რამდენად პირნათლად ასრულებს მომხმარებლის ავთენტიფიკაციას, თუ უნდა დაეყრდნოს აუდიტის დასკვნას?** |
| მომხამრებლის ძლიერი ავთენტიფიკაციის ვალდებულება ეკისრება იმ კომერციულ ბანკს თუ პროვაიდერს, რომლის მომხმარებელიცაა კონკრეტული პირი. კომერციული ბანკის/პროვაიდერის ვალდებულება არ არის შეამოწმოს რამდენად ასრულებს სხვა საგადახდო მომსახურების პროვაიდერი წესის მოთხოვნებს. |

|  |
| --- |
| 1. **რა იგულისხმება „ანგარიშგებით მიწოდებული (შეტყობინებული) თაღლითობის მაჩვენებლები“-ში (მუხლი 5.3.)?** |
| გთხოვთ იხილოთ წესის 21-ე მუხლი. |

**დროებითი/სამუდამო დაბლოკვა**

|  |
| --- |
| 1. **გთხოვთ, განმარტოთ დროებით ან სამუდამო დაბლოკვას შორის განსხვავება მცდელობების მაქსიმალურ რაოდენობასთან მიმართებაში.**   **შესაძლებელია ასეთი პროცედურა მოიაზრებდეს დისტანციურად აღდენას?** |
| დროებითი დაბლოკვის შემდეგ განბლოკვა ხდება ავტომატურად ბანკის მიერ განსაზღვრული წესით და განსაზღვრულ დროში.  რაც შეეხება სამუდამო ბლოკირებას, განბლოკვა არ ხდება ავტომატურად და საჭიროა მომხმარებლის მიერ ქმედება განსაბლოკად (მაგ. ფიზიკურად მისვლა ოფისში). ამას ბანკი განსაზღვრავს თავისი პროცედურებით თანმდევი რისკებიდან გამომდინარე.  მუდმივად დაბლოკვა როდის უნდა განხორციელდეს, ამას განსაზღვრავს პროვაიდერი წესის შესაბამისად. |

|  |
| --- |
| 1. **SMS კოდის არასწორედ შეყვანის შემთხვევაშიც უნდა იბლოკებოდეს მომხმარებელი?** |
| თუ კოდი არასწორად იქნა შეყვანილი და ავთენტიფიკაციის კოდის გენერირება წარუმატებელი იყო, წესის შესაბამისად უნდა დაიბლოკოს ელექტრონული საგადახდო ინსტრუმენტი ან/და ანგარიშებზე წვდომის ელექტრონული არხი. |

|  |
| --- |
| 1. **დღეს გვაქვს შემთხვევები ინტერნეტ ბანკში, რომ პირველ რიგში კლიენტებს ვუბლოკავთ ანგარიშს მყისიერი საფრთხის გათვალისწინებით და ამის შემდეგ ვატყობინებთ ხოლმე. ვფიქრობ ამის საშუალება უნდა გვქონდეს და შესაბამისად ჩამოყალიბდეს ფორმულირება, მაგალითად მოთხოვნას რომ დაემატოს „როცა შესაძლებელია“.** |
| წესში საუბარია ავთენტიფიკაციის მიმდევრობით წარუმატებელი მცდელობების მაქსიმალური რაოდენობის შემდეგ დროებით ან სამუდამო დაბლოკვაზე.  კითხვაში აღწერილი მაგალითში, არ არის საუბარი ავთენტიფიკაციის წარუმატებელ მცდელობებზე. |

|  |
| --- |
| 1. **წესი მიუთითებს, რომ ავთენტიფიკაციის მიმდევრობით წარუმატებელი მცდელობების მაქსიმალური რაოდენობა განსაზღვრული პერიოდისთვის არ უნდა აღემატებოდეს ხუთს. რას ნიშნავს დროის დადგენილი პერიოდითვის?** |
| საუბარია პროვაიდერის მიერ განსაზღვრულ პერიოდზე - „პროვაიდერის მიერ რისკზე დაფუძნებული მიდგომის საფუძველზე განსაზღვრული პერიოდისთვის“. |

|  |
| --- |
| 1. **დაბლოკვის შესახებ შეტყობინების გაგზავნა არ უნდა იყოს წინაპირობა დაბლოკვისთვის. შეტყობინება შეგვიძლია გავაგზავნოთ პოსტფაკტუმ? SMS საკმარისია თუ ფოსტით უნდა გაიგზავნოს მისამართზე შეტყობინება?** |
| როდესაც რამდენჯერმე დაიბლოკება „დროებით“, შეიძლება მომხმარებელს მიეწოდოს ინფორმაცია, რომ მონაცემების კიდევ ერთხელ შეცდომით(/წარუმატებელი) შეყვანა გამოიწვევს „სამუდამოდ“ დაბლოკვას.  წესი არ განსაზღვრავს შეტყობინების მიწოდების არხს. შესაბამისად, პროვაიდერი აირჩევს ეფექტურ გზას. |

|  |
| --- |
| 1. **რა პერიოდით ადრე უნდა მოხდეს შეტყობინება?**   **რა ფორმით? მე-5 მცდელობამდე უნდა შეატყობინოს? თუ ზოგადად მოხდეს მომხმარებლის ინფორმირება სანამ უშუალოდ წარუმატებელ მცდელობებს განახორციელებს?** |
| წინასწარი შეტყობინების ვალდებულება არის მხოლოდ სამუდამო დაბლოკვის შემთხვევაში, რომლის განბლოკვა ავტომატურ რეჟიმში არ მოხდება. წესი არ განსაზღვრავს ფორმას. ეს ფომა წინასწარ უნდა იყოს შეთანხმებული პროვაიდერსა და მომხმარებელს შორის.  რაც შეეხება „რა პერიოდით ადრე უნდა მოხდეს შეტყობინება“, წესი ადგენს რომ „საბოლოო დაბლოკვამდე“ უნდა მიეწოდოს ინფორმაცია მომხმარებელს რომ მისი წვდომა/საგადახდო ინსტრუმენტი დაიბლოკება სამუდამოდ. |

**დინამიური კავშირი**

|  |
| --- |
| 1. **მუხლი 7.1. საბარათე გადახდის ოპერაციას ეხება, თუ მხოლოდ გადარიცხვის ოპერაციას?** |
| მე-7 მუხლის მოთხოვნები ვრცელდება ყველა ელექტრონული გადახდის ოპერაციის ინიცირებაზე. კონკრეტულად საბარათე ოპერაციაზე დამატებითი მოთხოვნა განსაზღვრულია ამ მუხლის მე-3 პუნქტის „ა“ ქვეპუნქტით. |

|  |
| --- |
| 1. **მუხლი 7.1.ა - რა მომენტშია ვალდებული აჩვენოს ოპერაციის თანხისა და მიმღების შესახებ ინფორმაცია?**   „ა) საგადახდო მომსახურების პროვაიდერი ვალდებულია გადამხდელს აჩვენოს ოპერაციის თანხისა და მიმღების შესახებ ინფორმაცია;“ |
| მომხმარებელს უნდა ჰქონდეს საშუალება თავის მეირ შეყვანილი მონაცემები საბოლოოდ დათანხმებამდე გადაამოწმოს და შემდგომ დაეთანხმოს გადახდას. |

|  |
| --- |
| 1. **ბარათიდან ბარათზე გადარიცხვისას, მიმღების შესახებ კონკრეტულად რა ინფორმაცია უნდა იყოს იდენტიფიცირებული გადამხედილსთვის.** |
| მე-7 მუხლის პირველი პუნქტის „ა“ ქვეპუნქტში იგულისხმება, რომ საბოლოო დადასტურებამდე გადამხდელმა გადახედოს თავის მიერ მითითებულ ინფორმაციას. |

|  |
| --- |
| 1. **როდესაც მიმღების იდენტიფიცირება ვერ ხდება, მაგალითად მობილურის ნომერი, აქ შესაძლებელია ვაჩვენოთ, რომ მიმღები არის „ოპერატორი“, აბონენტი არის „5XX XXX XXX”.** |
| როდესაც გადახდა ხდება მობილურის ბალანსის შესავსებად, რა თქმა უნდა, გადახდის ოპერაციაში მიმღები არის მობილურის ოპერატორი.  მე-7 მუხლის პირველი პუნქტის „ა“ პუნქტის მიზანია, რომ საბოლოო დადასტურებამდე გამგზავნმა გადახედოს თავის მიერ მითითებულ ინფორმაციას (მათ შორის მობილურის ნომერს). |

|  |
| --- |
| 1. **მუხლი 7.1.ბ - იგულისხმება, რომ ავთენტიფიკაციის კოდთან ერთად, თანხა და მიმღები უნდა უჩანდეს სმს-ში?**   **მაგ. სახელი გვარი, 300 ლარი 751457? გთხოვთ, განგვიმარტოთ, თუ სხვა რამ იგულისხმება.**  **თითოეული გადახდის ოპერაციის შესრულების წინ მომხმარებლისთვის გაგზავნილი ერთჯერადი OTP კოდი (რომელიც აკმაყოფილებს ავთენტიფიკაციის ელემენტების კატეგორიას) საკმარისი არის ამ მოთხოვნის შესრულებისთვის?** |
| წესის მე-7 მუხლის პირველი პუნქტის მოთხოვნაში არ იგულისხმება SMS-ით გაგზავნილი გადახდის ოპერაციის შინაარსი. აღნიშნული პუნქტი გულისხმობს, რომ გადახდის განხორციელებამდე, დასტურის მიცემისას გადამხდელს უნდა ჰქონდეს საშუალება ნახოს მის მიერ შეყვანილი ინფორმაცია.  ასევე, „ბ“ ქვეპუნქტი ეხება ავთენტიფიკაციის კოდის, და არა ელემენტის, გენერირებას. |

|  |
| --- |
| 1. **გთხოვთ დაგვიზუსტოთ, რა იგულისხმება შემდეგ ჩანაწერში?**   **წესის მე-7 მუხლის პირველი ნაწილის „გ“ პუნქტის მიხედვით, “საგადახდო მომსახურების პროვაიდერის მიერ დადასტურებული ავთენტიფიკაციის კოდი უნდა შეესაბამებოდეს გადამხდელის მიერ დადასტურებულ თავდაპირველ გადახდის ოპერაციის თანხასა და მიმღებს;”** |
| პირველ რიგში, საყურადღებოა მე-7 მუხლის პირველი პუნქტის „ბ“ ქვეპუნქტი: „ავთენტიფიკაციის კოდი გენერირებული უნდა იყოს სპეციალურად გადამხდელის მიერ გადახდის ოპერაციის ინიციირებისას დადასტურებული გადახდის ოპერაციის თანხისთვის და მიმღებისთვის;“. აღნიშნული განსაზღვრავს, რომ ავთენტიფიკაციის კოდი აუცილებლად დაკავშირებული უნდა იყოს კონკრეტულ მიმღებთან და კონკრეტულ თანხასთან, ე.ი. კოდი ამ ინფორმაციიდან გამომდინარე სპეციფიკური და სპეციალურია. მოთხოვნების დაცვით კოდის გენერირების შემდგომ, პროვაიდერი ვალდებულია დაადასტუროს (მუხლი 7.1.“გ“) მხოლოდ ის ავთენტიფიკაციის კოდი, რომელიც კონკრეტული ოპერაციის ინიციირების ფარგლებში დაგენერირდა. ე.ი. თუ კოდი დაგენერირდა ოპერაციისთვის, სადაც მიმღებია „ა“, ხოლო, თანხა “X”, აღნიშნული კოდით პროვაიდერი ადასტურებს მხოლოდ შესაბამის ოპერაციას, და არა ოპერაციას მაგ. მიმღები „ა“-ს მიმართ და თანხის „Y“ ოდენობით. |

|  |
| --- |
| 1. **თუ ხდება ე.წ. batch გადახდები, აუცილებელია თუ არა მასში შემავალი ყოველი გადახდისთვის ძლიერი ავთენტიფიკაციის შესრულება?** |
| არ არის აუცილებელი. თუ გადამხდელი დაეთანხმა ერთი ან მეტი მიმღების მიმართ დისტანციური ელექტრონული გადახდის ოპერაციების პაკეტური ფაილის სახით შესრულებას, ავთენტიფიკაციის კოდი უნდა შეესაბამებოდეს მხოლოდ ამ გადახდის ოპერაციების პაკეტური ფაილის ჯამურ თანხას და მითითებულ მიმღებს/მიმღებებს. |

|  |
| --- |
| 1. **თუ პაკეტით თითოეული გადარიცხვა არ საჭიროებს ძლიერს ავტენტიფიკაციას, პაკეტური გადახდა იქნება მის გარეშე. თუ პაკეტში ერთი გადახდა საჭიროებს ძლიერს, მაშინ როგორ ვიქცვით?** |
| ასეთ შემთხვევაში აუცილებელია ძლიერი ავთენტიფიკაციის განხორციელება. შესაბამისად ავთენტიფიკაციის კოდი დაგენერირდება მთლიანი პაკეტისთვის. |

# **ავთენტიფიკაციის ელემენტების მიმართ მოთხოვნები**

|  |
| --- |
| 1. **ფლობის კატეგორიის ელემენტების არაუფლებამოსილი პირების მიერ გამოყენება.**   **ეს ნაწილი სრულად დამოკიდებულია გადამხდელზე, ფლობის კატეგორიის ელემენტების გამჟღავნების შეზღუდვა ვფიქრობთ შეუძლებელია.** |
| პროვაიდერი პასუხისმგებელია ფლობის კატეგორიის ელემენტად გამოიყენოს ისეთი „მოწყობილობები“, რომელთა მიმართ აქვს მაქსიმალური რწმუნება, რომ ამ მოწყობილობას იყენებს უფლებამოსილი მომხმარებელი. ასევე, დამატებითი ავთენტიფიკაციის ელემენტები უნდა აზღვევდეს, რომ ამ მოწყობილობას ვერ გამოიყენებს არაუფლებამოსილი პირი. |

|  |
| --- |
| 1. **შეგვიძლია თუ არა ე.წ. „eMail OTP“ მივაკუთვნოთ ფლობის კატეგორიას?** |
| დიახ, შესაძლებელია. გასათვალისწინებელია, რომ ელ. ფოსტაზე ერთჯერადი კოდის გაგზავნა უფრო მაღალი რისკის მატარებელია, ვიდრე მისი მობილურ ნომერზე გაგზავნა. როდესაც კოდი ელ. ფოსტაზე გაიგზავნება, სასურველია განსხვავებული მონიტორინგი განხორციელდეს, რათა მაქსიმალურად შემცირებული იქნეს რისკები და პროვაიდერიც დარწმუნდეს, რომ მომხმარებლის მიერ მოხდა კოდის მიღება. |

|  |
| --- |
| 1. **მუხლი 9.1. - როგორ უნდა მოხდეს ზომების შემუშავება ქუჩაში განლაგებულ ტერმინალებთან მიმართებაში.** |
| მუხლი ეხება მომხმარებლის (თავის ან პროვიადერის მიერ უზრუნველყოფილ) ელემენტებს, რომლებიც მიეკუთვნება ფლობის კატეგორიას. თვითმომსახურების კიოსკები (ისევე როგორც ბანკომატები) ვერ ჩაითვლება ფლობის კატეკორიის ელემენტად. |

|  |
| --- |
| 1. **ელემენტების დამოუკიდებლობა და მრავალფუნქციური ტექნიკური მოწყობილობა.**   შედის თუ არა ასეთ მოწყობილობაში მომხმარებლის კომპიუტერი და მობილური ტელეფონი? ხომ არ არსებობს ამ ზომების უფრო დეტალური აღწერა სახელმძღვანელოს სახით ან დოკუმენტაცია, რომელიც განმარტავს თუ რა ტექნიკური პარამეტრები მოიაზრება ამ ჩამონათვალში? |
| დიახ, შედის მობილური ტელეფონი, პლანშეტი, კომპიუტერი და ყველა ის მოწყობილობა რაც მრავალფუნქციურია.  ტექნოლოგიური ნეიტრალიტეტის პრინციპების დაცვის მიზნით, ასეთი რეკომენდაციები არ არის წარმოდგენილი. |

|  |
| --- |
| 1. **მუხლი 11.3.ა. - ერთი მოწყობილობისთვის ერთი სესიის გახსნა იგულისხმება?**   3. ამ მუხლის მე-2 პუნქტში განსაზღვრული ზომები უნდა აკმაყოფილებდეს ყველა შემდეგ პირობას:  ა) მრავალფუნქციურ ტექნიკურ მოწყობილობაში ჩაწერილი პროგრამული უზრუნველყოფის საშუალებით განცალკევებული უსაფრთხო შესრულების გარემოს გამოყენებას; |
| აქ იგულისხმება უსაფრთხოება როგორც hardware, ასევე software კუთხით. ევრო-რეგულაციაში ნეიტრალური ჩანაწერია და არ ზღუდავს პროგრამულ უზრუნველყოფას (თავდაპირველი ჩანაწერი მხოლოდ მოწყობილობას მოიაზრებდა, თუმცა მიღებამდე შეცვალეს).  მოწყობილობის მხრივ გულისხმობს: ტექნიკურად მოწყობილობას უნდა ჰქონდეს დამოუკიდებელი/ იზოლირებული აპლიკაციის პროცესინგის საშუალება/სივრცე, სადაც იმუშავებს (will run) მხოლოდ ეს კონკრეტული აპლიკაცია და ფიზიკურად ვერ მოხდება მასზე სხვა აპლიკაციების ზემოქმედება.  პროგრამული უზრუნველყოფის თვალსაზრისით, თავად აპლიკაცია იმგავარად უნდა იქნეს შემუშავებული, რომ შეუძლებელი იყოს მოწყობილობაში არსებული სხვა აპლიკაციების, მათ შორის, ვირუსების და ე.წ. malware-ის ზემოქმედება აპლიკაციაზე. ე.ი. დაცული იყოს ჩარევისგან. პარალელი რომ გავავლოთ, აპლიკაციას უნდა ჰქონდეს ე.წ. firewall ყველა სხვა აპლიკაციის/პროგრამული უზრუნველყოფის წინააღმდეგ. ამგვარად აპლიკაცია იმუშავებს ჩარევის გარეშე და დამოუკიდებლად (შესაბამისად, ვირუსი მაგ. ვერ შეცვლის მითითებულ ბენეფიციარს, ოდენობას, ვერ დააკოპირებს შეყვანილ მონაცემებს და ა.შ.). |

|  |
| --- |
| 1. **ანდროიდ პლატფორმაზე დაწერილი აპლიკაციებისთვის, მაგალითად თუ მომხმარებელმა დარუტა ანდროიდი, და შემდეგ ამის გამო მოხდა თაღლითობა. მხოლოდ გამაფრთხილებელი კამპანია თუ დაიცავს მომხმარებელს, რათა იცოდეს დარუტვა ნიშნავს, რომ მისი ანდროიდ პლატფორმა შესაძლოა გარე ზემოქმედების მსხვერპლი გახდეს.** |
| საკითხთან მიმართებაში, გთხოვთ, იხილოთ კითხვა 96-ის პასუხი.  ასევე, პროვაიდერმა თავად უნდა გადაწყვიტოს, წესთან შესაბამისობისთვის და უსაფრთხოების დასაცავად, მისცემს თუ არა მომხმარებელს აღნიშნულის შესაძლებლობას. თუმცა, რადგან ე.წ. „დარუთვა“ შეიცავს რისკებს, უსაფრთხოების მიზნებიდან გამომდინარე პროვაიდერს შეუძლია დანერგოს მექანიზმი, რომლითაც მობილური აპლიკაციის მიერ მოხდება ასეთი წვდომის დაფიქსირება. შედეგად შეუძლებელი იქნება აპლიკაციის ინსტალაცია კონრეტულ მოწობილობაზე ან არ ჩაირთვება აპლიკაცია.  მომხმარებლის ინფორმირება ზემოხსენებული რისკების შესახებ შესახებ ხელს შეუწყობს მის დაცვას. |

|  |
| --- |
| 1. **მუხლი 11.3.ბ. - რა მოთხოვნებია ამ (მომხმარებლისთვის მიწოდებული მოწყობილობისა და პროგრამული უზრუნველყოფის უცვლელობის დადგენა) მექანიზმებისთვის საჭირო, ან რამე სტანდარტი თუ არსებობს, რასაც უნდა ითვალისწინებდეს ეს მექანიზმები.** |
| ტექნოლოგიური ნეიტრალიტეტიდან გამომდინარე, წესი არ განსაზღვრავს კონკრეტულ სტანდარტს. პროვაიდერმა უნდა გაითვალისწინოს/გამოიყენოს საუკეთესო პრაქტიკა, რომელიც უზრუნველყოფს წესის მოთხოვნების შესრულებას. |

|  |
| --- |
| 1. **მუხლი 11.3.გ. – „შედეგების შემცირების მექანიზმში“ შეიძლება ჩაითვალოს მხოლოდ მომხმარებლის ინფორმირება?** |
| მომხმარებლის ინფორმირება საკმარისი არ არის. პროვაიდერმა თავის მხარესაც უნდა შეძლოს რისკების მიტიგაცია. |

**გამონაკლისები**

**ანგარიშზე წვდომა**

|  |
| --- |
| 1. **რას გულისხმობს „გასაზღვრული საგადახდო ანგარიშის ბალანსი“?** |
| მომხმარებლის მიერ მითითებულ (designated) კონრეტულ ანგარიშ(ებ)ზეა საუბარი. მომხმარებელმა წინასწარ უნდა მონიშნოს ანგარიშები, რომელთა ბალანსის და განხორციელებული ოპერაციების ნახვა სურს გამარტივებული წვდომის რეჟიმში. |

|  |
| --- |
| 1. **დეველოპმენტის კუთხით, რაც დამატებით ძალისხმევასთან იქნება დაკავშირებული და მომხმარებლის გამოცდილებას (ე.წ. UX) გაართულებს, ეს არის ძლიერი ავთენტიფიკაციის მეთოდის გამოყენება 3 თვეზე მეტი ვადის მონაცემების დათვალიერებისთვის. შესაძლებელია რომელიმე გამონაკლისისთ სარგებლობა?** |
| წესში გათვალისწინებულია დებულება, რომლის თანახმად, თუ მომხმარებლის მიერ განსაზღვრულ ერთ ან მეტ საგადახდო ანგარიშზე უკანასკნელი 90 კალენდარული დღის განმავლობაში შესრულებულ გადახდის ოპერაციების შესახებ ინფორმაციაზე წვდომა განხორციელდა მხოლოდ ცოდნის კატეგორიის ელემენტის გამოყენებით, პროვაიდერი უფლებამოსილია 90 კალენდარულ დღეზე მეტი პერიოდის ოპერაციებზე წვდომისთვის იმავე უწყვეტი სესიის ფარგლებში მომხმარებლის ძლიერი ავთენტიფიკაციისთვის ერთ-ერთ ელემენტად გამოიყენოს მომხმარებლის მიერ უკვე შეყვანილი ცოდნის კატეგორიის ეს ელემენტი და დაამატოს მხოლოდ ერთი ელემენტი (OTP, თითის ანაბეჭდი ან სხვა). |

|  |
| --- |
| 1. **საგადახდო ანგარიში „გადახდის ოპერაციის შესრულების წესის“ მიხედვით განიმარტება?**   **შესაძლებელია თუ არა ძლიერი ავთენტიფიკაციის გარეშეც - ხედვის რეჟიმში მომხმარებლებს ვაჩვენოთ ინფორმაცია ანაბრებსა და სესხებზე?** |
| წესი ვრცელდება მხოლოდ საგადახდო ანგარიშებზე. რაც შეეხება დეპოზიტის და სესხის ნახვის შესაძლებლობას, ეს არ არის შეზღუდული აღნიშნული წესით.  რეკომენდებულია, რომ ასეთ ანგარიშებზე ინფორმაციის ნახვა შესაძლებელი იყოს მხოლოდ ძლიერი ავთენტიფიკაციის გზით. |

|  |
| --- |
| 1. **მუხლი 12-ში ბარათზე ხელმისაწვდომი ნაშთის გაგებაც იგულისხმება? მაგალითად ვებით? მესიჯით?** |
| ბარათზე არსებული თანხა საგადახდო ანგარიშზეა, შესაბამისად ვებ-ით წვდომისას დაცული უნდა იყოს წესის მოთხოვნები.  SMS - არ არის ანგარიშზე ონლაინ რეჟიმში წვდომის საშუალება, შესაბამისად მასზე წესი არ ვრცელდება.  (3. ამ წესის მოქმედება ვრცელდება გადამხდელის მიერ: ა) დისტანციურად ონლაინ რეჟიმში თავის საგადახდო ანგარიშზე წვდომაზე;). |

**უკონტაქტო გადახდები**

|  |
| --- |
| 1. **თუ Visa-ს ექნა განსხვავებული ლიმიტი, Visa-ც მოვა შესაბამისობაში ამ ლიმიტებთან?** |
| ამ წესის მიზნებისთვის აუცილებელია მოთხოვნები შესრულდეს საგადახდო მომსახურების პროვაიდერების მიერ.  საქართველოს კანონმდებლობას აქვს უპირატესობა რომელიმე ორგანიზაციის წესებთან მიმართებაში. |

|  |
| --- |
| 1. **როგორ მოვიქცეთ ისეთ „ვენდინგ მანქანების“ შემთხვევაში, რომლებსაც არ გააჩნიათ კოდის ასაკრეფი ღილაკები? ამ აპარატებზე ვერ მოხდება პინის შეყვანა, თუ სწორედ ამ აპარატზე მოუწია მე-5 უკონტაქტო 150 ლარიანი ლიმიტის ქვემოთ ოპერაციამ. საჭიროა ამ დროს ძლიერი ავთენტიფიკაცია?** |
| ზოგადად, თუ ქმედება ექცევა წესის მოქმედების სფეროში და გამონაკლისში არ არის გათვალისწინებული, სავალდებულოა ძლიერი ავთენტიფიკაციის განხორციელება. თუმცა, დასახელებული შემთხვევისთვის, წესში სპეციალურად იქნა გათვალისწინებული, ჩანაწერი 10 ლარამდე გადახდების შესახებ. კერძოდ, 2025 წლის 1 იანვრამდე, პროვაიდერი უფლებამოსილია, 10 ლარამდე გადახდის ოპერაციები არ გაითვალისწინოს უკონტაქტო ოპერაციების მიზნებისთვის დათვლაში, თუ პროვაიდერის მიერ უკონტაქტო გადახდების მაქსიმალური რაოდენობა დღე-ღამის განმავლობაში შეზღუდულია 30-მდე. |

|  |
| --- |
| 1. **ვრცელდება თუ არა უკონტაქტო გადახდების შესახებ მუხლის შეზღუდვა Tap2Phone-ის ტიპის ტერმინალებზე (ანდროიდ ტელეფონი NFC-ის მხარდაჭერით, რომელზეც ჩაწერილია გადახდების მიღების ფუნქცია)?** |
| დიახ, ამ პროდუქტზეც გავრცელდება მე-13 მუხლის მოთხოვნები. |

|  |
| --- |
| 1. **საერთაშორისო საგადახდო სისტემების ლიმიტები თუ შეიცვალა ამ შემთხვევაში რომელი დოკუმენტით უნდა ვიხელმძღვანელოთ?** |
| საქართველოს კანონმდებლობას აქვს უპირატესობა რომელიმე ორგანიზაციის წესებთან მიმართებაში. |

|  |
| --- |
| 1. **ბარათის შემთხვევაში რას მოიცავს ძლიერი ავთენტიფიკაცია?**   **ასევე, ტექნოლოგიურად არის ძალიან რთული ბოლო გამოყენების კონტროლი, ვინაიდან ტრანზაქცია ხორციელდება ონლაინ რეჟიმში.** |
| ბარათის შემთხვევაში მოიცავს ბარათის პინს და ბარათის წამკითხველი მოწყობილობის მიერ წაკითხულ ბარათის მონაცემებს.  პინის გარეშე ოპერაციების კონტროლი შესაძლებელი უნდა იყოს ავტომატიზაციის საფუძველზე. |

|  |
| --- |
| 1. **მუხლი 13.ა და 13.ბ. - გაუგებარია რა იგულისხმება ამ შემთხვევაში?**   **თუ მომხმარებლის ძლიერი ავთენტიფიკაცია არ მომხდარა რაღაც პერიოდის მანძილზე (რა პერიოდი იგულისხმება) 150 ლარზე მეტი თანხის უკონტაქტოდ გატარების უფლება არ უნდა ქონდეს?** |
| ძლიერი ავთენტიკაციისგან თავისუფლდება სავაჭრო/მომსახურების ობიექტებში განხორციელებული უკონტაქტო გადახდები შემდეგი პირობების დაცვით  ა) უკონტაქტო ერთი ტრანზაქციის თანხა არ უნდა არემატებოდეს 150 ლარს და  მიყოლებით შესრულებული უკონტაქტო გადახდების მაქსიმალური თანხა არ უნდა აღემატებოდეს 600 ლარს ***(თუ მიყოლებით ძლიერი ავთენთიფიკაციის გარეშე შესრულებული ტრანზაქციების ჯამური თანხა 600 ლარს გადააჭარბებს, მოთხოვნილი უნდა იყოს ძლიერი ავთენთიფიკაცია. შემდეგომ ტრანზაქციებზე ისევ გავრცელდება გამონაკლისი)***  ბ) უკონტაქტო ერთი ტრანზაქციის თანხა არ უნდა არემატებოდეს 150 ლარს და  მიყოლებით შესრულებული უკონტაქტო გადახდების მაქსიმალური რაოდენობა არ უნდა იყოს 4-ზე მეტი. ***(თუ მიყოლებით ძლიერი ავთენთიფიკაციის გარეშე შესრულებული ტრანზაქციების რაოდენობა 4-ს გადააჭარბებს, მოთხოვნილი უნდა იყოს ძლიერი ავთენთიფიკაცია.*** ***შემდეგომ ტრანზაქციებზე ისევ გავრცელდება გამონაკლისი)*** |

|  |
| --- |
| 1. **ათვლა იწყება ბოლო ძლიერი ავთენტიფიკაციის გამოყენებით შესრულებული ტრანზაქციიდან და არ ნულდება დროის მიხედვით?** |
| აღნიშნული ჩანაწერი არ მოიცავს დროის პერიოდს, რის შემდეგ ძლიერი ავთენტიფიკაციის გარეშე შესრულებული ოპერაციების ხელახალი ათვლა იწყება.. |

|  |
| --- |
| 1. **უკონტაქტო მცირეფასიან გადახდებზეც არის გამონაკლისი?** |
| უკონტაქტო და ამავდროულად მცირეფასიან გადახდებთან მიმართებაში, განთვალისწინებულია 31-ე მუხლის მე-11 მუხლი. პროვაიდერი უფლებამოსილია, 10 ლარამდე გადახდის ოპერაციები არ გაითვალისწინოს უკონტაქტო ოპერაციების მიზნებისთვის ჯერადობის დათვლაში, თუ პროვაიდერის მიერ უკონტაქტო გადახდების მაქსიმალური რაოდენობა დღე-ღამის განმავლობაში შეზღუდულია 30-მდე. ამ უფლებამოსილებით სარგებლობა შესაძლებელია 2025 წლის 1 იანვრამდე. |

|  |
| --- |
| 1. **მცირემოცულობიანი გადახდის ოპერაციისა და სავაჭრო/მომსახურების ობიექტებში უკონტაქტო გადახდებისთვის გათვალისწინებული მეთოდებიდან პროვაიდერი ირჩევს, რომელს გამოიყენებს თუ ეროვნული ბანკი განსაზღვრავს?** |
| თუ გადახდა უკონტაქტოა, მაშინ პროვაიდერმა უნდა იხელმძღვანელოს უკონტაქტო გადახდებისთვის დადგენილი მოთხოვნებით. |

**მგზავრობისა და პარკირების საფასური**

|  |
| --- |
| 1. **მუხლი 14 - სრულყოფილია ამ გამონაკლისების ჩამონთავალი? სხვა სერვისებიც ხომ არ განიხილება?**   **გთხოვთ, განმარტოთ, ჩანაწერით იგულისხმება თუ არა, რომ თუ გადამხდელი იხდის სმპ საშუალებით ტრანსაპორტის (დასაკონკრეტებელია ტრანსპორტის სახეობა) და პარკირების (როგორი პარკირების სერვისის?) საფასურს, ის არ ექვემდებარება ავთენტიფიკაციას.** |
| დიახ, ჩამონათვალი ამომწურავია. იგულისხმება მუნიციპალური ტრანსპორტი.  Exemptions also exist for contactless payments and transactions for small amounts, and particular types of payments such as urban transport fares or parking fees[[2]](#footnote-2).  For instance, the EBA has added a new exemption for unattended terminals for fares related to transport and parking services, ***since it may not be proportionate and may also not be in the general public interest for operational (e.g. to avoid queues and potential accidents at toll gates) or security reasons (e.g. the risk of shoulder surfing)[[3]](#footnote-3).*** |

**სანდო ბენეფიციარი**

|  |
| --- |
| 1. **სანდო ბენეფიციარად შეიძლება ჩაითვალოს თუ არა მხოლოდ ფიზიკური პირი?** |
| სანდო ბენეფიციარი შესაძლოა იყოს როგორც ფიზიკური, ასევე იურიდიული პირი, ასევე, სხვა ორგანიზაციული წარმონაქმნიც, რომელიც არ არის იურიდიული პირი. |

|  |
| --- |
| 1. **ძლიერი ავთენტიფიკაციით ერთი გადახდა საფუძველია თუ არა მომავალში მომხმარებლის სანდო ბენეფიციარად მისაჩნევად?** |
| ოპერაციების ისტორიიდან შესრულებული გადარიცხვის ხელმეორედ განხორციელება არ წარმოადგენს მიმღების სანდოდ მიჩნევის კრიტერიუმს. |

|  |
| --- |
| 1. **მნიშვნელოვანია, რომ ბენეფიციარად მიჩნეული იყოს არა მხოლოდ ანგარიშის ნომერი, არამედ მის უკან მდგომი ფიზიკური/იურიდიული პირი, რადგან ბენეფიციარის იდენტიფიკატორი არის არა ერთი, არამედ რამდენიმე ანგარიშის ნომერი, ასევე შეიძლება იყოს მობილური ნომერი, პირადი ნომერი ან სხვა რაიმე მსგავსი იდენტიფიკატორი, რომლითაც კლიენტს ოპერაციის შესრულება შეუძლია.** |
| წესით სანდო ბენეფიციარის ცნება შეზღუდული არ არის ანგარიშის ნომერზე.  მნიშვნელოვანია რომ მომხმარებლის მიერ სანდო ბენეფიციარის განსაზღვრისას მას ჰქონდეს სრული ინფორმაცია რა რეკვიზიტებით განხორციელდება მომდევნო ოპერაციები. |

|  |
| --- |
| 1. **შესაძლებელია თუ არა პირის პირადი საბანკო ან/და საბარათე ანგარიშის დამატება საბდო ბენეფიციარად?** |
| დიახ, შესაძლებელია. აქვე, თუ პირის ანგარიშები ერთ პროვაიდერთანაა, შესაძლებელია გამონაკლისით სარგებლობა (მე-17 მუხლი) და ოპერაციის ძლიერი ავთენტიფიკაციის გარეშე ინიციირება. |

|  |
| --- |
| 1. **რამდენად იქნება შესაძლებელი, რომ მომხმარებელს ყველა მისი ისტორიული ბენეფიციარი ერთიანი სიის სახით ვუჩვენოთ, სანდო ბენეფიციარები ავარჩევინოთ და SCA-ის ორი კომპონენტის კომბინაციით დავადასტურებინოთ?** |
| შესაძლებელია მომხმარებლისთვის ღია სიის შეთავაზება, სადაც მომხმარებელი თავად მონიშნავს სასურველ ბენეფიციარებს. სია არ უნდა იყოს პაკეტის სახით, რომელსაც მომხმარებელი ერთიანად ეთანხმება ან არ ეთანხმება. მას უნდა ჰქონდეს ინდივიდუალურად მონიშვნის/არჩევის შესაძლებლობა. |

|  |
| --- |
| 1. **სანდო ბენეფიციარები - ამ ეტაპზე ციფრულ არხებში ყოველ ახალ ბენეფიციართან გადარიცხვისას მომხმარებელს ტრანზაქციას ვადასტურებინებთ ერთჯერადი კოდით (OTP) და განმეორებით გადარიცხვაზე კოდს აღარ ვთხოვთ. გვაინტერესებს, არსებული პროცესი რამდენად ჩაჯდება ახალ რეგულაციებში? ასევე, თუ ხელახლა „გასანდოება“ მოგვიწევს, რაიმე ვადა უნდა ჰქონდეს თუ სამუდამოა?** |
| თქვენ მიერ აღწერილი გადაწყვეტა არ დააკმაყოფილებს წესის მოთხოვნებს. წესის მე-15 მუხლის (სანდო ბენეფიციარების შესახებ) თანახმად, ინიციირებამდე მიმღები წინასწარ (24 საათით ადრე მაინც) უნდა იყოს დამატებული გადამხდელის მიერ შექმნილ სანდო ბენეფიციარების ჩამონათვალში. ამასთან, გთხოვთ, გაითვალისწინოთ ამავე მუხლის დებულებები, მათ შორის ის, რომ მომხმარებელს ინფორმაცია უნდა მიეწოდოს მიმღების სანდო ბენეფიციარად დამატებისა და მისი შედეგის შესახებ, რის საფუძველზეც მომხმარებელს ექნება გაცნობიერებული გადაწყვეტილების მიღების შესაძლებლობა. რაც შეეხება ვადას, წესი მას არ განსაზღვრავს და პროვაიდერი უფლებამოსილია ამ გამონაკლისით ისარგებლოს და, რისკზე დაფუძნებული მიდგომიდან გამომდინარე, სურვილის/საჭიროების შემთხვევაში, თავად განსაზღვროს ბენეფიციარის „სანდოობის“ ვადა. |

|  |
| --- |
| 1. **როდესაც მომხმარებელი ციფრული არხიდან აინიცირებს გადარიცხვას, შესაძლებელია თუ არა, რომ გადარიცხვის ე.წ. “review” გვერდზე დაეთანხმოს ფიზიკური პირის ან კომპანიის სანდო კონტაქტად დამატებას და აღარ მოუხდეს მისი ცალკე OTP კოდით დადასტურება? წინააღმდეგ შემთხვევაში მომხმარებლის გამოცდილება ძალიან გართულდება.** |
| სანდო ბენეფიციარად დამატება უნდა განხორციელდეს მომხმარებლის ძლიერი ავთენტიფიკაციით. შესაძლებელია ერთი ძლიერი ავთენტიფიკაციით მოხდეს ორი ქმედება - ინიციირება და სანდო ბენეფიციარად განსაზღვრა. აქვე, გთხოვთ გაითვალსიწინოთ, რომ მომხმარებლისთვის ცნობილი უნდა იყოს განსხვავება სანდო ბენეფიციარად დამატებასა და მონაცემის (ე.წ. შაბლონის) შენახვას შორის. ასევე, წესის შესაბამისად მომხმარებელმა უნდა იცოდეს რა შედეგს გამოიწვევს მისი კონკრეტული ქმედება. |

|  |
| --- |
| 1. **დასაზუსტებელია: ინტერნეტ და მობაილ ბანკში არსებული შაბლონები იგულისხმება? ბენეფიციარში იგულისხმება კომუნალურები, მობილურის შევსება და ა.შ.?** |
| ე.წ. „შაბლონი“ არ ნიშნავს „სანდო ბენეფიციარს“.  მომხმარებელს უნდა ჰქონდეს ცალკე საშუალება განსაზღვროს მისთვის სანდო მიმღებების რეკვიზიტები (მაგ. მობილურის ოპერატორის, თელასის და შვილის).  შაბლონი არის მოსახერხებელი გადარიცხვის შესასრულებლად და არ არის აუცილებელი ყველა შაბლონში ბენეფიციარი იყოს „სანდო“.  ასევე გასათვალისწინებელია, რომ საგადახდო მომსახურების პროვაიდერი უფლებამოსილია, რისკზე დაფუძნებული მიდგომის საფუძველზე, ასევე, მომხმარებლებისგან მიღებული საჩივრების გათვალისწინებით განსაზღვროს ბენეფიციარები, რომლებთან მიმართებაში ის არ ისარგებლებს ამ მუხლით გათვალისწინებული გამონაკლისით. |

|  |
| --- |
| 1. **გვჭირდება განმარტება, კლიენტი ძლიერ ავთენტიფიკაციას იყენებს მაგ: ინტ ბანკინგში შესასვლელად და ვთქვათ შექმნა ბენეფიციარი. შემდეგ ამ ბენეფიციართან რომ განახორციელოს გადარიცხვა, მას შეუძლია ეს დადასტურების გარეშე განახორციელოს ნებისმიერ თანხაზე?** |
| ოპერაციების განსახორციელებლად ინტერნეტ-ბანკში შესვლას სჭირდება ძლიერი ავთენტიფიკაცია. შემდგომ:  ა) „სანდო ბენეფიციარის“ შექმნას სჭირდება ძლიერი ავთენტიფიკაცია.  ბ) უკვე შექმნილი „სანდო ბენეფიციარის“ სასარგებლოდ გადარიცხვას არ სჭირდება ძლიერი ავთენტიფიკაცია. |

|  |
| --- |
| 1. **მომხმარებლებისთვის “White List” ფუნქციონალის შეთავაზება კატეგორიის გადახდისათვის მისაღები იქნება?** |
| არა. შეთავაზება შეიძლება მოხდეს, თუმცა არა კატეგორიის ჩამონათვალის, არამედ კონკრეტულად ბენეფიციარების სიის სახით (სია არ იქნება მბოჭავი და მომხმარებელს უნდა შეეძლოს დაეთანხმოს სიიდან თუნდაც ერთს). |

|  |
| --- |
| 1. **სანდო ბენეფიციარისთვის 500 ლარზე მეტის გადახდა შეიძლება?** |
| დიახ, ძლიერი ავთენტიფიკაციის გარეშე შესაძლებელია სანდო ბენეფიციარის მიმართ გადახდა განხორციელდეს 500 ლარზე მეტ თანხაზეც. აღნიშნული ლიმიტი ეხება დაბალრისკიანი ოპერაციების შესახებ გამონაკლისს. |

**განმეორებადი/პერიოდული გადახდები**

|  |
| --- |
| 1. **მუხლი 16.1. - გთხოვთ, განმარტოთ ტერმინი „სერია“.** |
| განმეორებადი/პერიოდული (Reccuring) გადახდების მაგალითია სესხის დასაფარად ყოველთვიური გადასახადი, სადარბაზოს მოვლისთვის ყოველთვიური ფიქსირებული ოდენობის თანხის გადასახადი და სხვა. სერია არის ასეთი გადახდების ერთობლიობა, რომელიც შემოფარგლულია ბოლო გადახდის ვადით ან მუდმივად ხდება გადახდა. |

|  |
| --- |
| 1. **განმეორებადი/პერიოდული გადახდის ოპერაციების სერია უნდა იყოს ერთი და იმავე თანხაზე და ერთი და იმავე მიმღების სასარგელოდ. ეს შეზღუდვა გახდება ბარიერი პირდაპირი დებეტის პროდუქტისთვის.** |
| გარდა ფიქსირებული თანხის გადახდებისა, ასევე დაშვებულია ისეთი პერიოდული გადახდების განხორციელება, სადაც მომხმარებელს ცალსახად აქვს განსაზღვრული შესასრულებელი ოპერაციების თანხის ოდენობის გამოთვლის პრინციპი.  რაც შეეხება საყოფაცხოვრებო გადახდებს, გთხოვთ იხილოთ წესის 31-ე მუხლის მე-8 პუნქტი. |

|  |
| --- |
| 1. **მუხლი 16.2. - ეს შეიძლება შეეხოს ელ. კომერციით რექარინგ გადახდებს?**   **თითოეული მერჩანტის დონეზე უნდა იყოს თუ სისტემურ დონეზე?**  **თუ მაგალითად კომუნალურების ყოველთვიური ავტომატური დაფარვის მოდულია ჩართული და თვიურად გადასახდელი თანხა განსხვავდება, ამ შემთხვევაში სავალდებულოა ძლიერი ავთენტიფიკაცია?** |
| ელექტრონული კომერციის ოპერაციების შემთხვევებში, როდესაც ოპერაცია ხორციელდება მომხმარებელის მიერ დამახსოვრებული ბარათის მონაცემებით, აუცილებლად არ მოიაზრება წესით დადგენილ გამონაკლის გადახდებში. თუ მომხმარებელი აინიცირებს გადახდას, ძლიერი ავთენტიფიკაცია უნდა განხორციელდეს.  რაც შეეხება საყოფაცხოვრებო გადახდებს, გთხოვთ იხილოთ წესის 31-ე მუხლის მე-8 პუნქტი. |

|  |
| --- |
| 1. **როგორ მოვიქცეთ, როცა ავტომატურ შეგროვებას ვახდენთ საბანკო ოპერაციების პარალელურად, მაგ. საბავშვო ანაბარზე? თანხა ცვლადია, შეადგენს შესრულებული ოპერაციის გარკვეულ პროცენტს. ასევე, შეგროვება ხდება დღის ბოლოს მერჩანტთან.** |
| ასეთი შემთხვევებისთვის გათვალისწინებული იქნა წესის მე-16 მუხლის მე-4 პუნქტი, რომლის მიხედვითაც არ გამოიყენოს მომხმარებლის ძლიერი ავთენტიფიკაცია სერიაში შემავალი ყველა მომდევნო გადახდის ოპერაციის ინიციირებისთვის, თუ განმეორებადი/პერიოდული გადახდის ოპერაციის მიმღები უცვლელია და მომხმარებელს ცალსახად აქვს განსაზღვრული შესასრულებელი ოპერაციების თანხის ოდენობის გამოთვლის პრინციპი. |

|  |
| --- |
| 1. **თუ გადახდა არ არის ინიცირებული გადამხდელის მიერ, ასეთ გადახდებზე ეს წესი არ ვრცელდება. შესაბამისად გაურკვეველია რას ეხება მე-16 მუხლი.** |
| აღნიშნული მუხლი ეხება მომხმარებლის მიერ ინიციირებულ გადადის ოპერაციებს, რომლებიც განხორციელდება გარკვეული პერიოდულობით, ასევე მიმღები და თანხა უცვლელია ან მომხმარებელს ცალსახად აქვს განსაზღვრული შესასრულებელი ოპერაციების თანხის ოდენობის გამოთვლის პრინციპი. მომხმარებელი პირველ ჯერზე გასცემს თანხმობას, რომ შესრულდეს მომავალი ოპერაციები.  გთხოვთ, იხილოთ ამონარიდი EBA-ს კითხვა პასუხიდან: Payment transactions that are not initiated by the payer but by the payee only are therefore not subject to strong customer authentication (SCA) to the extent that these transactions are initiated without any interaction or involvement of the payer. (Question ID: 2018\_4131)  <https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4131> |

|  |
| --- |
| 1. **განვადების ტიპის ოპერაციები ასევე უნდა შევიდეს გამონაკლისში, როდესაც კლიენტი თავიდან ეთანხმება სრული თანხის გადახდას, შეთანხმებული გრაფიკით. მაგალითად სადაზღვევო პოლისის განვადება.** |
| აღნიშნული განსაზღვრულია წესის მე-16 მუხლში. |

|  |
| --- |
| 1. **დაზღვევის თანხა ხშირად ფიქსირებულია უცხოურ ვალურტაში, მაგრამ ირიცხება ლარში იმ დღეს არსებული ოფიციალური კურსით. მოექცევა თუ არა ასეთი გადახდა გამონაკლისში?** |
| დიახ, ის მოექცევა გამონაკლისში. აღნიშნული შემთხვევისთვის გათვალისწინებულია მე-16 მუხლის მე-3 პუნქტი, რომლის თანახმად, პროვაიდერმა ძლიერ ავთენტიფიკაციამდე მომხმარებლისთვის ცნობილი უნდა გახადოს კონვერტაციის კურსი (კურსის წყარო). |

|  |
| --- |
| 1. **თუ გადასარიცხი თანხა არის ექვივალენტ ლარში, მაგალითად, უნდა გადაირიცხოს ყოველთვე 100 დოლარის შესაბამისი ექვვივალენტი ლარი. ამ შემთხვევაში კურსის გამო ოპერაციის თანხა იქნება განსხვავებული ყოველი ოპერაციისას. შეგვიძლია თუ არა ჩავთვალოთ რომ კლიენტის დავალება 100 დოლარის ექვივალენტი ლარის გადარიცხვაზე თანხა უცვლელია?** |
| დიახ. ამ შემთხვევაში დამატებით უნდა დაკმაყოფილდეს წესის მე-16 მუხლის მე-3 პუნქტის დებულება. |

|  |
| --- |
| 1. **თუ გადამხდელი ყოველთვიურად (სერიულად) იხდის ელექტროენერგიის ერთი და იგივე საფასურს, სერვისის გადახდისთვის მომხმარებელი არ ექვემდებარება ავთენტიფიკაციას, ხოლო თუ თანხის მოცულობა იცვლება - უნდა მოხდეს ავთენტიფიკაცია?** |
| საყოფაცხოვრებო მომსახურებების გადახდებთან დაკავშირებით იხილეთ წესის 31-ე მუხლის მე-8 პუნქტი. |

**ერთი და იმავე პირის ანგარიშებს შორის საკრედიტო გადარიცხვა**

|  |
| --- |
| 1. **მუხლი 17 - საკრედიტო გადარიცხვის გარდა ერთსა და იმავე პირს შორის სხვა ტიპის რა გადარიცხვა არსებობს?**   **გთხოვთ, განმარტოთ, რამ გამოიწვია აქ ამ ტერმინის ჩამატება?** |
| წესი ვრცელდება მხოლოდ მომხმარებლის **მიერ ინიცირებულ ოპერაციაზე.** განსაკუთრებული დატვირთვა ტერმინი „საკრედიტო“-ს დამატებას არ აქვს, გარდა ზემოაღნიშნულისა. |

|  |
| --- |
| 1. **მხოლოდ საკრედიტო გადარიცხვები? აქ იგულისხმება ყველა სახის ანგარიში და ფულადი გადარიცხვა თუ რეალურად მხოლოდ საკრედიტო ანგარიშებს შორის გადარიცხვაზეა საუბარი.** |
| წესი ვრცელდება **საგადახდო** ანგარიშებიდან მომხმარებლის **მიერ ინიცირებულ ოპერაციაზე**. |

**დაბალი რისკის გადახდები**

|  |
| --- |
| 1. **საბარათე გადახდის დროს მომხმარებლის მიერ შეიძლება დაფიქსირდეს ძლიერი ავთენტიფიკაციის მოხსნის მოთხოვნა გარკვეული დროით ან სამუდამოდ. ასეთ შემთხვევაში შეგვიძლია ოპერაცია მივიჩნიოთ დაბალ რისკიანად?** |
| პირველ რიგში, ოპერაციის დაბალრისკიანობას აფასებს თავად პროვაიდერი და არა მომხმარებელი. გარდა ამისა, გთხოვთ, გაითვალისწინოთ, რომ მომხმარებელს არ უნდა ჰქონდეს საშუალება უარი თქვას ძლიერი ავთენტიფიკაციის განხორციელებაზე. ასევე, პროვაიდერი ვალდებულია ძლიერი ავთენტიფიკაცია განახორციელოს წესის შესაბამისად და განსაზღვრულ შემთხვევებში, ხოლო მომხმარებლის უარი ასეთ პროცედურაზე და რისკის თავის თავზე აღება არ არის წესთან შესაბამისი. |

|  |
| --- |
| 1. **წესით მოითხოვება ე.წ. Behavior analysis. გთხოვთ განგვიმარტოთ, რა პერიოდის ანალიზი მიიჩნევა მიზანშეწონილად?** |
| წესი არ განსაზღვრავს პერიოდს. დამოკიდებულია მომხმარებელზე, შესრულებული გადახდების რაოდენობაზე და ა.შ. პროვიადერმა თავად უნდა მიიღოს დასაბუთებული გადაწყვეტა. პერიოდი რაც უფრო დიდია, მით უფრო სწორი იქნება ქცევითი ანალიზის შედეგი. |

|  |
| --- |
| 1. **რის მიხედვით განისაზღვრება მაღალი რისკის ადგილმდებარეობა? იგულისხმება ოფშორული ზონები?** |
| იგულისხმება, მაგალითად, ქვეყნები სადაც ბარათის თარლითობის მაღალი მაჩვენებელია. პროვაიდერს უნდა გააჩნდეს თავისი ანალიზის საფუძველზე ასეთი ადგილმდებარეობების ჩამონათვალი. |

|  |
| --- |
| 1. **რას ნიშნავს „მაღალი რისკის მიმღები?“** |
| ისეთ მიმღებს, რომელიც სტატისტიკურად ფროდის მაღალი მაჩვენებელით ხასიათდება ან არსებობს თაღლითობის მაღალი რისკი. |

|  |
| --- |
| 1. **რას გულისხმობს გამონაკლისით სარგებლობისთვის ოპერაციის თანხის ზღვრული ოდენობა (დანართში)?** |
| აღნიშნული გულისხმობს, რომ შესაბამისი გამონაკლისით (მუხლი 20. გადახდის ოპერაციის რისკის ანალიზი) სარგებლობა დასაშვებია არაუმეტეს 500 ლარის ფარგლებში, თუ პროვაიდერი აკმაყოფილებს იმავე დანართში განსაზღვრულ პროცენტულ მაჩვენებლებს. |

|  |
| --- |
| 1. **თუ ბანკი არ სარგებლობს გამონაკლისით ამ შემთხვევაში არ აწვდის ეროვნულ ბანკს ინფორმაციას გამონაკლისის შეწყვეტაზე?** |
| დიახ, თუ პროვაიდერი არ სარგებლობს დაბალრისკიანი ოპერაციების შესახებ გამონაკლისით (წესის მე-20 მუხლი), ის შესაბამისად ვერ მიაწვდის აღნიშნულთან დაკავშირებით რამე ინფორმაციას. ასევე, წესის მიხედვით, ასეთი ინფორმაციის მიწოდების ვალდებულება განსაზღვულია მხოლოდ ხსენებული გამონაკლისისთვის. |

|  |
| --- |
| 1. **ტრანზაქციის რისკის შეფასების მიდგომა თუ ანაცვლებს გამონაკლისების პირობების ან სხვა წესების დაცვის ვალდებულებას?** |
| წესის შესაბამისად, გამონაკლისები, მათ შორის, რისკის შეფასებასთან დაკავშირებული, პროვაიდერს აძლევს უფლებას არ მოითხოვოს ძლიერი ავთენტიფიკაცია. ოპერაციის დაბალრისკიანად შეფასება არ გამორიცხავს წესში და, ზოგადად, სამართლებრივ აქტებში გათვალისწინებულ ვალდებულებებს/პასუხისმგებლობას, მათ შორის, მომხმარებლის წინაშე არსებულ პროვაიდერის ვალდებულებებს. |

|  |
| --- |
| 1. **მუხლი 20.2.გ. - არის რაიმე შეზღუდვა ანალიტიკური მოდელის არჩევაში, ან ქცევის „ნორმალურობის“ დადგენისათვის კალკულაციის ან რეკალკულაციის დროით პარამეტრებში?** |
| პროვაიდერს არ აქვს შეზრუდვა ანალიტიკური მოდელის არჩევაში. |

|  |
| --- |
| 1. **მუხლი 20.3.ა. - ახალ მომხმარებლებზე როგორ უნდა მოხდეს ხარჯვის მოდელის განსაზღვრა?** |
| ისტორიული მონაცემების დაგროვებამდე რთული იქნება ახალი კლიეტის სრულყოფილად შეფასება. |

|  |
| --- |
| 1. **მუხლი 20.3.გ. - გეოგრაფიული ადგილმდებარეობის დადგენა არ იქნება ზუსტი, რადგან მომხმარებელს შეუძლია VPN-სერვისი ჩართოს, მაგალითად, ანდროიდზე და ისე დალოგინდეს.** |
| ეს ერთ-ერთ კომპონენტია. ეს კომპონენტი უნდა გამოიყენოს პროვაიდერმა, სადაც შესაძლებელია. |

|  |
| --- |
| 1. **საგადახდო მომსახურების პროვაიდერი ვალდებულია საქართველოს ეროვნულ ბანკს მიაწოდოს იმ ზომების აღწერა, რომლების გატარებასაც ის გეგმავს ცხრილში მითითებულ მაჩვენებელთან შესაბამისობის აღსადგენად. რა ვადებში და როგორი წესით უნდა მიაწოდოს პროვაიდერმა ხსენებული ინფორმაცია ეროვნულ ბანკს?** |
| ვადა, ფორმა ან მიწოდების დამატებითი წესი განსაზღვრული არ არის. რაც შეეხება ვადას, დროულად მიწოდება, სავარაუდოდ, პროვაიდერის ინტერესებში იქნება. |

|  |
| --- |
| 1. **20.4. - როგორ უნდა განისაზღვროს რისკის დონის მინიჭება და შესაბამისი ქულები?** |
| მონიტორინგის სისტემები ძირითადად აგებულია ტრანზაქციისთვის ქულის მინიჭებაზე, რომელიც განისაზღვრება სხვადასხვა ფაქტორებზე (ამ წესისთვის ფაქტორები ჩამოთვლილია მე-20 მუხლის მე-3 პუნქტში) |

|  |
| --- |
| 1. **მუხლი 21.3 - კვარტლის ბოლოს მგდომარეობით, თუ კვარტლის განმავლობაში?** |
| Rolling quarterly basis (90 days) - ანუ მაგ. ივნისში სრულდება „როლინგ“ პერიოდი მარტი-აპრილი-მაისისთვის. ხოლო, ივლისში დასრულდება აპრილი-მაისი-ივნისისთვის (თუმცა „backsight“ პერიოდად აიღება 90 დღე (რადგან თვეებში გაანსვავებული დღეებია და ამან არ გამოიწვიოს მნიშვნელოვანი სხვაობა)). |

|  |
| --- |
| 1. **მუხლი 21.4. - დაანგარიშებამდე უნდა მოხდეს შეთანხმება სებ-თან, თუ პოსტფაქტუმ შემოწმება?** |
| დოკუმენტირებული მეთოდოლოგიის ეროვნული ბანკისთვის მიწოდებაზეა საუბარი.  შეთანხმების ვალდებულებას წესი არ ადგენს. |

|  |
| --- |
| 1. **მუხლი 22.1 - მიზანშეწონილია, რომ გარკევული ვადა დაწესდეს: თუ დაანგარიშება მოხდება მომდევნო კვარტლის მაქსიმუმ მე-10 სამუშაო დღეს, შეტყობინებაც ამ ვადასთან უნდა იყოს დაკავშირებული.** |
| სწორედ კითხვაში ხსენებულ ვადასთან აკავშირებს წესიც:  **თუ ამ წესის დანართის ცხრილში მითითებული რომელიმე ტიპის გადახდის ოპერაციასთან მიმართებაში დაანგარიშებული თაღლითობის მაჩვენებლები**, რომლების მონიტორინგსაც საგადახდო მომსახურების პროვაიდერი ახორციელებს, აღემატება ამავე ცხრილში განსაზღვრულ შესაბამის მაჩვენებლებს, **საგადახდო მომსახურების პროვაიდერი**, რომელიც სარგებლობს ამ წესის მე-20 მუხლში მითითებული გამონაკლისით, **ვალდებულია აღნიშნულის შესახებ დაუყოვნებლივ შეატყობინოს საქართველოს ეროვნულ ბანკს.** |

|  |
| --- |
| 1. **შესაძლებელია თუ არა დისტანციურ არხზე შესვლისას, პაროლის შეყვანისას კლიენტისთვის შეყვანილი პაროლის ჩვენება?** |
| გთხოვთ, იხილოთ წესის 24-ე მუხლის პირველი და მე-2 პუნქტები. აქვე ყურადღებას ვამახვილებთ ამავე მუხლის მე-2 პუნქტის „ა“ ქვეპუნქტზე, რომლის თანახმად, ავთენტიფიკაციის განხორციელებისას უსაფრთხოების პერსონიფიცირებული მახასიათებლები უნდა იყოს შენიღბულად ნაჩვენები და მომხმარებლის მიერ მათი შეყვანისას შეუძლებელი უნდა იყოს მათი სრულად წაკითხვა.  შესაბამისად, დაუშვებელია პაროლის კლიენტისთვის ჩვენება. ასევე, დაუშვებელია ის შემთხვევაც, როდესაც პაროლი შეყვანისას ავტომატურად შენიღბულია, თუმცა კლიენტს აქვს საშუალება ღილაკზე დაჭერით გამოაჩინოს სრული პაროლი. |

|  |
| --- |
| 1. **გთხოვთ, დაგვიკონკრეტოთ, თუ უნდა მოხდეს მომხმარებლის სახელის (username) შენიღბული ჩვენება, ვინადაინ აღნიშნული წარმოადგენს პერსონიფიცირებულ მახასიათებელს.** |
| მომხმარებლის სახელი არ წარმოადგენს ავთენტიფიკაციის ელემენტს და შენიღბვის შესახებ მოთხოვნა მასზე არ ვრცელდება. თუმცა, თუ პროვაიდერი გადაწყვეტს, აღნიშნული შესაძლებლობა შეზღუდული არ არის. |

|  |
| --- |
| 1. **ვისთვის უნდა იყოს და ვისთვის არა შენიღბულად ნაჩვენები უსაფრთხოების პერსონიფიცირებული მახასიათებლები?** |
| ეს მოთხოვნა ვრცელდება უსაფრთხოების პერსონიფიცირებულ მახასიათებლებზე და არ ხდება განსხვავება სუბიექტების მიხედვით. შეყვანისას ვერავინ უნდა ხედავდეს ასეთ მონაცემებს სრულად. |

|  |
| --- |
| 1. **გთხოვთ, დაგვიკონკრეტოთ რა იგულისხმება საიდუმლო კრიპტოგრაფიულ მასალაში.** |
| იგულისხმება, მაგალითად, დახურული გასაღები (PKI – private key infrastructure), ასევე, ისეთი მასალა, რომლითაც შესაძლებელია კრიპტოგრაფიულად დაცული ინფორმაციის წაკითხვა. |

|  |
| --- |
| 1. **რა ხდება როცა ემიტენტი უცხოელია (არ აქვს SCA-ს ვალდებულბა თავის ქვეყანაში) და მისი მომხმარებელი საქართველოში იხდის, და პირიქით, საქართველოში გამოშვებული ბარათი გამოიყენება ისეთ ქვეყანაში, სადაც SCA არ მოითხოვება?** |
| აღნიშნული შემთხვევებისთვის, წესში გათვალისწინებული დებულებები, რომლებიც განსაზღვრული ვადით იძლევა მომსახურების შეუფერხებლად მიწოდებისთვის შესაძლებლობას. კერძოდ, უცხო ქვეყნის საგადახდო მომსახურების პროვაიდერის მიერ გამოშვებულ საბარათე ინსტრუმენტებთან მიმართებაში, საგადახდო მომსახურების პროვაიდერი 2025 წლის 1 იანვრამდე უფლებამოსილია რისკზე დაფუძნებული მიდგომის საფუძველზე თავად გადაწყვიტოს გამოიყენოს თუ არა მომხმარებლის მიმართ ძლიერი ავთენტიფიკაცია. ამავე თარიღამდე, ემიტენტი უფლებამოსილია უცხოური ექვაირერის მომსახურებაში მყოფი სავაჭრო/მომსახურების ობიექტებთან მისი მომხმარებლების მიერ განხორციელებულ საბარათე ოპერაციებთან მიმართებაში გადაწყვეტილება მიიღოს რისკზე დაფუძნებული მიდგომის საფუძველზე. |

|  |
| --- |
| 1. **გათვალისწინებული იქნება შეუსაბამო ბარათების ჩანაცვლებისთვის გარკვეული ვადა? აუცილებელია პროვაიდერებს ჰქონდეთ ვადა ბარათების დასაბეჭდად და ჩასანაცვლებლად.** |
| წესის გარდამავალ დებულებებში (31-ე მუხლის მე-6 პუნქტი) განსაზღვრულია ვადა - 2021 წლის 1 სექტემბერი, რომლის განმავლობაშიც წესთან შეუსაბამო ბარათები უნდა ჩანაცვლდეს. |

|  |
| --- |
| 1. **როგორ ხდება პროგრამული უზრუნველყოფის განადგურება? ასევე, მომხმარებლისთვის გადაცემული ტექნიკური მოწყობილობის განადგურება ან გადადგურებაზე კონტროლი როგორ განხორციელდება? (მაგ.: მომხმარებლისთვის უცნობია აღნიშნული მოწყობილობის ადგილმდებარეობა/დაგაკრგა)** |
| განადგურება, თუ არ იგეგმება მისი ხელმეორედ გადაცემა, უნდა მოხდეს იმგვარად, რომ შეუძლებელი იყოს მესამე პირის მიერ მისი გამოყენება. დაკარგვის შემთხვევაში შეუძლებელია მისი განადგურება, რა შემთხვევაშიც მოხდება მისი პროგრამულად დეაქტივაცია. |

|  |
| --- |
| 1. **გთხოვთ, დაგვიკონკრეტოთ რა იგულისხმება უკვე გამოყენებულ მოწყობილობაში (მაგ.:მომხმარებლის მიერ უკან დაბრუნებული დიჯი პასი)** |
| მომხამრებლის მიერ გამოყენებული და დაბრუნებული მოწყობილობა, მათ შორის, დიჯი პასის მოწყობილობა. |

**გარდამავალი დებულებები**

|  |
| --- |
| 1. **წესით შეიზღუდა უკონტაქტო ბარათების გამოშვება, თუმცა რაც ამ თარიღამდე დაიბეჭდა და ვადიანია, განაგრძობს მუშაობას?**   **წესის შესაბამისად შეიზღუდა თუ არა უჩიპო ბარათებით ოპერაციების შესრულება ბანკომატსა და პოს ტერმინალზე? რამდენადაც ფლობის კატეგორიის ელემენტებში მონაწილეობს მხოლოდ ჩიპიანი ბარათები და მოხდება მხოლოდ ცოდნის კატეგორიის ელემენტის - პინის გამოყენება.** |
| წესი არ ზღუდავს უკონტაქტო ტექნოლოგიის ბარათების გამოშვებასა და გამოყენებას. შეზღუდულია ისეთი ბარათების გამოყენება, რომელიც ვერ აკმაყოფილებს წესის მოთხოვნებს. პირველ რიგში, ასეთი ბარათი არის უჩიპო, მაგნიტურ-ზოლიანი საგადახდო ბარათი. ასევე, აღსანიშნავია, რომ SDA ტექნოლოგიით მოქმედი ჩიპიანი ბარათი ვერ დააკმაყოფილებს წესის მოთხოვნებს.  რაც შეეხება უკვე გამოშვებული შეუსაბამო ბარათების მოქმედებას, წესი განსაზღვრავს 2021 წლის 1 სექტემბრამდე მათი ჩანაცვლების ვალდებულებას. |

|  |
| --- |
| 1. **გარდამავალ დებულებაში საუბარია შეუსაბამო ბარათების ჩანაცვლებაზე და ვადაზე. თუმცა, აქამდე შეგვიძლია უკვე დაბეჭდილი ბარათები, რომლებიც არ შეესაბამება, ჩავუშვათ მიმოქცევაში მათ ამოწურვამდე?** |
| დაუშვებელია. წესის ამოქმედების შემდეგ პროვაიდერი ვალდებულია, გამოუშვას მხოლოდ ისეთი საბარათე ინსტრუმენტები, რომლებიც სრულად უზრუნველყოფს ამ წესის მოთხოვნებთან შესაბამისობას. |

|  |
| --- |
| 1. **თუ წესის ამოქმედების შემდეგ გამოვიყენებთ ერთ ელემენტს 3D კოდის სახით, ხოლო უცხოურ მერჩანტს არ ექნება გააქტიურებული 3D კოდით ავთენტიფიკაციის სისტემა, ასეთ შემთხვევაში პროვაიდერის მიერ გამოშვებულ ბარათებს უნდა შევუზღუდოთ უცხოურ საიტებზე ოპერაციის შესრულების შესაძლებლობა?** |
| არა, ასეთ შემთხვევაში შესაძლებელია გარდამავალი დებულებით სარგებლობა. კერძოდ, 2025 წლის 1 იანვრამდე ემიტენტი უფლებამოსილია უცხოური ექვაირერის მომსახურებაში მყოფი სავაჭრო/მომსახურების ობიექტებთან მისი მომხმარებლების მიერ განხორციელებულ საბარათე ოპერაციებთან მიმართებაში იმოქმედოს რისკზე დაფუძნებული მიდგომის საფუძველზე. შესაბამისად, პროვაიდერის გადასაწყვეტია, რა მიდგომა ექნება კითხვაში ხსენებული შემთხვევისთვის. |

|  |
| --- |
| 1. **ვებ-გვერდის მეშვეობით შეთავაზებული საგადახდო მომსახურების შესახებ 31-ე მუხლის მე-10 პუნქტში იგულისხმება აზარტული თამაშობის (ე.წ. გემბლინგის) ორგანიზატორის ვებ-გვერდიც?** |
| არა, იგულისხმება საგადახდო მომსახურების პროვაიდერების და არ იგულისხმება აზარტული თამაშობის (ე.წ. გემბლინგის) ორგანიზატორის ვებ-გვერდები. |

|  |
| --- |
| 1. **როდესაც სერვისი გადაცემულია არაპროვაიდერებზე (მაგ. აზარტული თამაშობების ორგანიზატორზე). ასეთ პირებს ძლიერი ავთენტიფიკაციის ვალდებულება არ ეხება და მათი საიტიდან ხდება თანხის შემოტანა პროვაიდერის მომხმარებლის საფულის ანგარიშზე. ასეთ დროს როგორ უნდა შესრულდეს ძლიერი ავთენტიფიკაცია?** |
| თუ ოპერაციის ინიციირება ხდება საგადახდო მომსახურების პროვაიდერის საფულედან, მაშინ მომხმარებელმა საფულეზე წვდომისთვის უნდა გაიაროს ძლიერი ავთენტიფიკაცია.  თუ ოპერაციის ინიციირება ხდება აზარტული თამაშობების ორგანიზატორის ვებ-გვერდიდან, ეს ოპერაცია განიხილება როგორც, მაგალითად, თვითმომსახურების კიოსკის საშუალებით საფულეს შევსება. |

|  |
| --- |
| 1. **31-ე მუხლის მე-8 პუნქტში საუბარია საყოფაცხოვრებო მომსახურების საფასურის გადახდაზე. როგორ განიმარტება საყოფაცხოვრებო მომსახურება?** |
| გადახდის ოპერაციის შესრულების წესი მოიცავს მის განმარტებას.  საყოფაცხოვრებო მომსახურების გადასახადია ელექტროენერგიის, გაზის, წყლის, დასუფთავების და სატელეკომუნიკაციო მომსახურებისათვის გადასახადი. |

|  |
| --- |
| 1. **როგორ მოვიქცეთ, იურიდიული პირების მიერ კომუნალურ გადახდებთან მიმართებით (რომლებიც უმეტესად აღემატება 500 ლარს), როდესაც მონიტორინგის მექანიზმი დაინერგება?** |
| საყოფაცხოვრებო მომსახურების ორგანიზაციების სასარგებლოდ გადახდები მოწესრიგებულია 31-ე მუხლის მე-8 პუნქტში. ამ პუნქტით გათვალისწინებულ შემთხვევაში, მონიტორინგის მექანიზმის მიმართ არ მოქმედებს წესის მე-20 მუხლით განსაზღვრული გადახდის ოპერაციის თანხობრივი სიდიდიდან გამომდინარე მოთხოვნები. შესაბამისად, არ შეფერხდება 500 ლარზე მეტი თანხის გადახდები. |

1. კითხვაზე პასუხი დაზუსტდა 2023 წლის იანვარში. [↑](#footnote-ref-1)
2. <http://europa.eu/rapid/press-release_IP-17-4928_en.htm> [↑](#footnote-ref-2)
3. EBA Final Report, EBA/RTS/2017/02, გვ. 10, კომენტარი 25, <https://eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf> [↑](#footnote-ref-3)