**მოთხოვნები მონიტორინგის სისტემის მიმართ**

**ძლიერი ავტენტიფიკაციის წესთან შესაბამისობიდან გამომდინარე**

მონიტორინგის სისტემა უნდა უზრუნველყოფდეს ძლიერი ავთენთიფიკაციის წესთან PSD2 ევრო დირექტივებთან შესაბამისობას და ასევე საქართველოს ეროვნული ბანკის მიერ 2020 წლის 2 სექტემბერს დამტკიცებულ მომხმარებლის ძლიერი ავთენტიფიკაციის წესთან და საქართველოს კანონი პერსონალურ მონაცემთა დაცვის შესახებ შესაბამისობას.

მონიტორინგის სისტემის არსებობის ძირითადი დანიშნულებაა არსებობდეს უფრო უსაფრთხო ეკოსისტემა მომხმარებელსა და ბანკს შორის ნებისმიერი კომუნიკაციის დროს და მათ შორის გათვალისწინებული იყოს შემდეგი:

* ძლიერი ავთენტიფიკაციის მექანიზმები;
* მალვეარის აღმოჩენის და მათზე რეაგირების მექანიზმები;
* რისკების ანალიზის მექანიზმები, რომელიც შესაძლებლობას იძლევა გამოვლინდეს თაღლითური ტრანზაქციები და მოხდეს მათი შემცირება/მიტიგაცია დროის რეალურ რეჟიმში.

სისტემა უნდა იძლეოდეს საშუალებას არ მოითხოვოს ძლიერი ავთენტიფიკაციის გამოყენება განსაზღვრული და შეზღუდული პირობების შესაბამისად, რისკის დონის, გადახდის ოპერაციის ოდენობისა და განმეორების და მისი შესრულებისათვის გამოყენებული გადახდის არხის საფუძველზე.

სისტემა უნდა იძლეოდეს საშუალებას ქცევითი ბიომეტრიისა (მოწყობილობის ხელში ჭერის კუთხე; სიმბოლოების აკრეფის სიჩქარე, ღილაკებზე დაჭერის ხანგრძლივობა) და მოწყობილობის ფლობის შეფასება (რაც დასტურდება მოწყობილობის მიერ ხელმოწერის გენერირებით (hardware or software token); აპლიკაცია ან ე.წ. ბრაუზერი, რომლების ფლობა დასტურდება მათი მოწყობილობასთან დაკავშირებით) მოახდინოს ტექნოლოგიების მეშვეობით იმისათვის, რომ შესაძლებელი იყოს ძლიერი ავთენტიფიკაციის გამოყენება ფლობა და უნიკალურობის ელემენტებზე დაყრდნობით.

სისტემა უნდა გააჩნდეს მექანიზმები რომლებიც ხელს უშლის მომხმარებლის გაყალბებას და მანიპულირებას და ასევე შესაძლებელს ხდის დაადგინოს განხორციელდა თუ არა ფიშინგი. შესაძლებელი უნდა იყოს ისეთი მექანიზმების ინტეგრირება, რომელიც დაადგენს იმ მცდელობებს, რომლებიც განხორციელდა საგადახდო მომსახურების პროვაიდერის უსაფრთხოების გვერდის ავლით.

გადახდის ოპერაციების მონიტორინგის მექანიზმი უნდა ითვალისწინებდეს, სულ მცირე, რისკზე დაფუძნებულ შემდეგ ფაქტორებს:

ა) კომპრომეტირებული ან/და მოპარული ავთენტიფიკაციის ელემენტების ჩამონათვალს;

ბ) თითოეული გადახდის ოპერაციის თანხას;

გ) თაღლითობის ცნობილ სცენარებს, რომლებსაც შესაძლოა ადგილი ჰქონდეს საგადახდო მომსახურების განხორციელებისას;

დ) ავთენტიფიკაციის პროცესის თითოეულ სესიაში შეფერხების ან/და დაზიანების გამომწვევი, ასევე ინფორმაციაზე არაუფლებამოსილი წვდომისთვის განკუთვნილი ფარული პროგრამული უზრუნველყოფის არსებობის ნიშნებს;

ე) თუ წვდომის ტექნიკური მოწყობილობა ან პროგრამული უზრუნველყოფა მომხმარებლისთვის საგადახდო მომსახურების პროვაიდერის მიერ არის მიწოდებული, მომხმარებლის მიერ მათი გამოყენების, მათ შორის, უჩვეულო გამოყენების აქტივობის ჩანაწერებს.

**ტრანზაქციის მონიტორინგის მექანიზმი:**

დროის რეალურ რეჟიმში უნდა იძლეოდეს საუალებას გამოავლინოს არაავტორიზებული ან თაღლითური გადახდის ოპერაციები რათა დაცული იყოს უსაფრთხოების ზომები.

ეს მექანიზმები უნდა ემყარებოდეს საგადახდო ოპერაციების ანალიზს იმ ელემენტების გათვალისწინებით, რომლებიც დამახასიათებელია საგადახდო მომსახურების მომხმარებლისთვის პერსონალური უსაფრთხოების მახასიათებლების ჩვეულ/ნორმალურ პირობებში გამოყენებისას.

ტრანზაქციის მონიტორინგის მექანიზმები უნდა იძლეოდეს საშუალებას დროის რეალურ რეჟიმში განახორციელოს რისკების ანალიზი რათა დაადგინოს:

ა)გადამხდელის ხარჯვისა და ქცევის უჩვეულო თავისებურება;

ბ) გადამხდელის ტექნიკურ მოწყობილობაზე ან პროგრამულ უზრუნველყოფაზე წვდომის შესახებ უჩვეულო ინფორმაცია;

გ) ავთენტიფიკაციის განხორციელების არცერთ სესიაში შეფერხების ან/და დაზიანების გამომწვევი, ასევე ინფორმაციაზე არაუფლებამოსილი წვდომისთვის განკუთვნილი ფარული პროგრამული უზრუნველყოფის არსებობა;

დ) საგადახდო მომსახურების თაღლითობის ცნობილი სცენარები;

ე) გადამხდელის უჩვეულო ადგილმდებარეობა;

ვ) მიმღების მაღალი რისკის შემცველი ადგილმდებარეობა.

მექანიზმების არსებობა, რომელიც რისკზე დაფუძნებული მიდგომის საფუძველზე მოახდენს შემდეგი ფაქტორების გათვალისწინებას:

ა) საგადახდო მომსახურების კონკრეტული მომხმარებლისთვის დამახასიათებელი ხარჯვის მოდელი;

ბ) საგადახდო მომსახურების პროვაიდერის ყოველი მომხმარებლის გადახდის ოპერაციების ისტორია;

გ) თუ წვდომის ტექნიკური მოწყობილობა ან პროგრამული უზრუნველყოფა საგადახდო მომსახურების პროვაიდერის მიერაა მიწოდებული, გადახდის ოპერაციის მომენტში გადამხდელისა და მიმღების ადგილმდებარეობა;

დ) მომხმარებლის გადახდის ოპერაციების ისტორიასთან მიმართებაში ამავე მომხმარებლის გადახდის უჩვეულო მოდელის გამოვლენა.

**მოთხოვნები ფლობის ელემენტების დაცულობაასთან დაკავშირებით.**

სისტემა უნდა იძლეოდეს საშუალებას ძლიერი ავთენტიფიკაციის მიზნებისთბის ფლობის ელემენტად მიჩნეული ელემენტები დაცული იყოს არაუფლებამოსილი მხარეების მიერ გამოიყენებისგან რათა თავიდან იყოს აცილებული ამ ელემენტების გამრავლება/რეპლიკაცია.

**მოთხოვნები უნიკალურობის ელემენტებთან დაკავშირებული მოწყობილობების და პროგრამული უზრუნველყოფის დაცულობასთან დაკავშირებით.**

სისტემა უნდა იძლეოდეს რისკების შემცირების საშუალებას არაუფლებამოსილი პირების მიერ ძლიერი ავთენტიფიკაციის მიზნებისთვის უნიკალურობის იმ ელემენტების მოპოვებასთან დაკავშირებით, რომელთა წაკითხვა ხორციელდება გადამხდელისთვის მიწოდებული წვდომის ტექნიკური მოწყობილობისა და პროგრამული უზრუნველყოფის მიერ. რათა თავიდან იქნეს აცილებული მოწყობილობებსა და პროგრამულ უზრუნველყოფაზე არაუფლებამოსილი წვდომით ამ ელემენტების არაუფლებამოსილი გამოყენება.

სულ მცირე, უზრუნველყოფილი უნდა იყოს მოწყობილობებისა და პროგრამული უზრუნველყოფის მიერ არაუფლებამოსილი პირების გადამხდელად ავთენტიფიკაციის მნიშვნელოვნად დაბალი ალბათობა.

**მოთხოვნები ელემენტების დამოუკიდებლობასთან დაკავშირებით.**

სისტემა უნდა იძლეოდეს საშუალებას დაცული იყოს ძლიერი ავთენთიფიკაციისთვის გამოყენებული ელემენტების დამოუკიდებლობა. კერძოდ: უნდა იყოს გამოყენებული ისეთი ტექნოლოგიები, ალგორითმები და პარამეტრები, რომ ერთ-ერთი ელემენტის კომპრომეტირების შედეგად სხვა ელემენტების საიმედოობა ეჭვის ქვეშ არ დადგეს.

ასევე, თუ მომხმარებლის ძლიერი ავთენტიფიკაციის რომელიმე ელემენტი ან ავთენტიფიკაციის კოდი გამოყენებულია მრავალფუნქციური ტექნიკური მოწყობილობიდან, შემცირებულ იქნეს ასეთი მოწყობილობის კომპრომეტირებით წარმოშობილი რისკები.

ამ მიზნისთვის განსაზღვრული ზომები ერთდროულად უნდა მოიცავდეს შემდეგს:

ა) მრავალფუნქციურ ტექნიკურ მოწყობილობაში ჩაწერილი პროგრამული უზრუნველყოფის საშუალებით განცალკევებული უსაფრთხო შესრულების გარემოს გამოყენებას;

ბ) მექანიზმებს, რათა პროვაიდერი დარწმუნდეს, რომ გადამხდელის ან მესამე მხარის მიერ არ მომხდარა მომხმარებლისთვის მიწოდებული მოწყობილობის ან პროგრამული უზრუნველყოფის მოდიფიკაცია/ცვლილება;

გ) თუ ადგილი ჰქონდა მომხმარებლისთვის მიწოდებული მოწყობილობის ან პროგრამული უზრუნველყოფის მოდიფიკაციას/ცვლილებას - აღნიშნულიდან გამომდინარე შედეგების შემცირების მექანიზმებს.

**მოთხოვნები უსაფრთხოების პერსონიფიცირებული მახასიათებლების შექმნასთან და გადაცემასთან.**

მექანიზმები, რომლებიც უზრუნველყოფენ შემცირებული იყოს არაუფლებამოსილი გამოყენების რისკები, რომლებიც შესაძლოა გამოწვეული იყოს უსაფრთხოების პერსონიფიცირებული მახასიათებლების, ავთენტიფიკაციის მოწყობილობების და პროგრამული უზრუნველყოფის, გადამხდელისთვის მიწოდებამდე მათი დაკარგვით, მოპარვით ან ასლის დამზადებით.

**მოთხოვნები უსაფრთხოების პერსონიფიცირებული მახასიათებლების, ავთენტიფიკაციის მოწყობილობების და პროგრამული უზრუნველყოფის მიწოდებასთან დაკავშირებით**

მექანიზმები რომლებიც გამოყენებული იქნება უსაფრთხოების პერსონიფიცირებული მახასიათებლების, ავთენტიფიკაციის მოწყობილობების და პროგრამული უზრუნველყოფის მომხმარებლისათვის დაცულად მიწოდებისათვის უნდა ითვალისწინებდეს შემდეგ მოთხოვნებს და ზომებს: მიწოდებასთან დ

ა) ეფექტური და დაცული მიწოდების მექანიზმები, რომლებიც უზრუნველყოფს უსაფრთხოების პერსონიფიცირებული მახასიათებლების, ავთენტიფიკაციის მოწყობილობებისა და პროგრამული უზრუნველყოფის საგადახდო მომსახურების უფლებამოსილი მომხმარებლისთვის მიწოდებას;

ბ) მექანიზმები, რომლებიც საგადახდო მომსახურების პროვაიდერს საშუალებას აძლევს შეამოწმოს მომხმარებელთან ინტერნეტის საშუალებით მიწოდებული ავთენტიფიკაციის პროგრამული უზრუნველყოფის უცვლელობა;

გ) ზომები იმ შემთხვევისთვის, თუ უსაფრთხოების პერსონიფიცირებული მახასიათებლების მიწოდება არ ხდება საგადახდო მომსახურების პროვაიდერის ოფისებში, ან ხდება დისტანციური არხის მეშვეობით, და ერთდროულად დაცულია შემდეგი მოთხოვნები:

გ.ა) თუ მიწოდება ხდება ერთი და იმავე არხის მეშვეობით, არც ერთ არაუფლებამოსილ მხარეს არ შეუძლია ერთზე მეტი უსაფრთხოების პერსონიფიცირებული მახასიათებლის, ავთენტიფიკაციის მოწყობილობის ან პროგრამული უზრუნველყოფის პარამეტრის მიღება;

გ.ბ) მიწოდებული უსაფრთხოების პერსონიფიცირებული მახასიათებლები, ავთენტიფიკაციის მოწყობილობები ან პროგრამული უზრუნველყოფა გამოყენებამდე მოითხოვს აქტივაციას.

დ) ზომები, რომლებიც უსაფრთხოების პერსონიფიცირებული მახასიათებლების, ავთენტიფიკაციის მოწყობილობების ან პროგრამული უზრუნველყოფის პირველად გამოყენებამდე აქტივაციის საჭიროების შემთხვევაში უზრუნველყოფს აქტივაციის პროცესის დაცულ გარემოში განხორციელებას.

**ტექნიკური სპეციფიკაცია:**

შეთავაზებული გადაწყვეტილება უნდა იყოს ინტეგრირებადი და გამოყენებადი შემდეგ ტიპის აპლიკაციებში:

Web Application

React, .Net, .Net core

Mobile Application

IOS, Android

React Native

აგრეთვე, გადაწყვეტილებას უნდა ჰქონდეს API ან ინტეგრაციის სხვა საშუალებები. მოცემული API ან ინტეგრაციის საშუალება, როგორც მინიმუმ, უნდა იძლეოდეს გადაწყვეტილების (Software Solution) მიერ დაგენერირებული ყველა რეპორტის ინტეგრირებას ბანკის ერთიან რეპორტების სისტემაში.

* **კომპანიამ უნდა წარმოადგინოს შესაბამისობის სერტიფიკატი / დოკუმენტაცია.**
* **იმპლიმენტაციის ფასი ერთჯერადი და ყოველწლიური (ასეთის არსებოსბის შემთხვევაში) გადასახადი.**