Gücləndirilmiş müştəri autentifikasiyası: hüquqi tənzimləmə və tətbiq problemləri

Jalə Kərimli[*]

Annotasiya

Son dövrlərdə rəqəmsal ödəniş xidmətlərinin geniş yayılması nəticəsində bu əməliyyatların təhlükəsizliyinin təmin edilməsi aktuallıq kəsb edən məsələlərdən birinə çevrilmişdir. Bu kontekstdə gücləndirilmiş müştəri autentifikasiyası (bundan sonra – GMA) ödənişlərin təhlükəsizliyinin artırılmasında mühüm rol oynayır. Bununla belə, GMA-nın tətbiqi autentifikasiya elementlərinin düzgün müəyyənləşdirilməsi, müxtəlif texnoloji vasitələrin hüquqi qiymətləndirilməsi, autentifikasiyadan istisnaların əsaslandırılması və əməliyyat risklərinin qiymətləndirilməsi ilə bağlı hüquqi suallar yaradır. Məqalədə GMA-nın hüquqi və praktiki aspektləri Azərbaycan Respublikasının qanunvericiliyi, Avropa İttifaqının İkinci Ödəniş Xidmətləri Direktivi (PSD2), müvafiq Tənzimləyici Texniki Standartlar (RTS) və Avropa Bank Təşkilatının (EBA) yanaşmaları əsasında müqayisəli şəkildə təhlil edilir. Tədqiqat çərçivəsində autentifikasiya elementlərinin müstəqilliyi, kart rekvizitləri, birdəfəlik parollar və biometrik məlumatlar kimi vasitələrin GMA tələblərinə uyğunluğu, eləcə də autentifikasiyadan istisnaların hüquqi əsasları araşdırılır. Həmçinin aşağı riskli əməliyyatların müəyyən edilməsi, risk göstəricilərinin monitorinqi və ödəniş xidməti təchizatçılarının bu prosesdəki rolu nəzərdən keçirilir. Təhlil nəticəsində milli tənzimləmənin praktiki tətbiqində hüquqi müəyyənliyin artırılmasına ehtiyac olduğu müəyyən edilir. Bu baxımdan GMA elementlərinin müəyyənləşdirilməsi üzrə daha konkret meyarların hazırlanması, müvafiq tələblərin tətbiqinə dair praktiki izahların verilməsi, istisnaların tətbiqi şərtlərinin aydınlaşdırılması, monitorinq mexanizmlərinin təkmilləşdirilməsi, eləcə də ödəniş xidməti təchizatçıları arasında risk məlumatlarının mübadiləsinin gücləndirilməsi təklif olunur.

Abstract

In recent years, the widespread adoption of digital payment services has made ensuring the security of these transactions an increasingly important issue. In this context, strong customer authentication (hereinafter SCA) plays an important role in enhancing payment security. However, the implementation of SCA raises legal questions concerning the proper identification of authentication elements, the legal assessment of different technological means, the justification of exemptions from SCA and the assessment of transaction risks. The article provides a comparative analysis of the legal and practical aspects of SCA on the basis of the legislation of the Republic of Azerbaijan, the European Union's Second Payment Services Directive, the relevant Regulatory Technical Standards and the approaches of the European Banking Authority. The study examines the independence of authentication elements, the compliance of means such as card credentials, one-time passwords and biometric data with SCA requirements, as well as the legal grounds for exemptions from SCA. It also considers the identification of low-risk transactions, the monitoring of risk indicators and the role of payment service providers in this process. The analysis finds that there is a need to increase legal certainty in the practical application of the national framework. In this regard, it is proposed to develop more specific criteria and practical guidance for identifying SCA elements, to clarify the conditions for applying exemptions,

[*] Bonn Universiteti, Hüquq magistr ixtisasının məzunu.

to improve risk-based monitoring mechanisms and to strengthen the exchange of risk information among payment service providers.

MÜNDƏRİCAT

Giriş....349
I. GMA-nın elementləri və onların tətbiq xüsusiyyətləri....351
A. "Bildiyi" elementi....352
B. "Sahiblik" elementi....354
C. "Məxsusluq" elementi....360
D. Elementlərin müstəqilliyi prinsipi....361
II. GMA-nın tətbiqində istisna hallar: milli qanunvericilik və beynəlxalq yanaşma....363
A. Azərbaycan Respublikasının GMA Qaydasına əsasən istisnalar....363
B. RTS-də nəzərdə tutulan əlavə istisnalar: Azərbaycan qanunvericiliyi ilə müqayisəli təhlil....372
III. Monitorinq mexanizmi necə tənzimlənməli və aşağı riskli əməliyyatlar hansılardır?....375
IV. GMA institutunun təkmilləşdirilməsinə dair təkliflər....377
A. GMA elementlərinin müəyyən edilməsi....378
B. GMA-nın tətbiqinə dair vahid izah və praktiki rəhbərliyin hazırlanması....378
C. Risk əsaslı monitorinqin və nəzarət mexanizmlərinin təkmilləşdirilməsi....379
D. GMA və onun istisnalarının tətbiqində ödəniş xidməti təchizatçılarının funksiyalarının fərqləndirilməsi....380
Nəticə....381

Giriş

Rəqəmsal iqtisadiyyatın sürətlə inkişafı və elektron ticarətin genişlənməsi müasir maliyyə sistemlərində ödəniş əməliyyatlarının təhlükəsizliyinin təmin edilməsini daha da vacib etmişdir. Xüsusilə 2020-ci ildə dünyada baş vermiş fövqəladə sanitar-epidemioloji vəziyyət nəticəsində elektron ticarətin həcmi əhəmiyyətli dərəcədə artmış, onlayn pərakəndə satışların ümumi pərakəndə satışdakı payı da nəzərəçarpacaq şəkildə yüksəlmişdir.[1] Bu artım rəqəmsal mühitdə

[1] UNCTAD, COVID-19 and E-commerce: A Global Review, 11, § 1.2. Burada bax: https://unctad.org/system/files/official-document/dtlstict2020d13_en_0.pdf (son baxış 13 sentyabr 2026); *həmçinin bax:* Danaja Fabcic, Strong Customer Authentication in Online

onlayn ödəniş sistemlərinin inkişafına olan tələbatın daha da artmasına səbəb olmuşdur. Buna paralel olaraq, elektron ticarətin genişlənməsi nəticəsində rəqəmsal mühitdə dələduzluq və kibercinayətkarlıq riskləri də artmışdır.[2] Bu səbəbdən bir çox ölkələrdə və beynəlxalq maliyyə qurumlarında bu halların qarşısının alınması üçün təhlükəsizlik tədbirlərinin gücləndirilməsinə xüsusi önəm verilir. Bu tədbirlərdən biri də GMA-nın tətbiqinə başlanılmasıdır.

GMA müştərinin kimliyinin təsdiqlənməsi üçün bir neçə müstəqil elementə əsaslanan autentifikasiya mexanizmidir. Azərbaycan qanunvericiliyində GMA-nın anlayışı və hüquqi əsasları "Ödəniş xidmətləri və ödəniş sistemləri haqqında" Azərbaycan Respublikası Qanununun 35-ci maddəsində təsbit edilmişdir.[3] Həmin normada Mərkəzi Bankın normativ xarakterli aktları ilə müəyyənləşdirilmiş digər hallara da istinad edilir. Həmçinin ödənişlərin təhlükəsizliyini artırmaq və ödəniş əməliyyatlarında dələduzluq riskini azaltmaq məqsədi ilə 2024-cü ildə Azərbaycan Respublikasının Mərkəzi Bankının İdarə Heyətinin qərarı ilə təsdiqlənmiş "Gücləndirilmiş müştəri autentifikasiyasının tətbiqi Qaydası"na (bundan sonra – Qayda) uyğun olaraq GMA-ya dair tələblər müəyyən edilib.[4] Sözügedən Qayda 2026-cı il yanvar ayından etibarən elektron ticarət də daxil olmaqla ödəniş əməliyyatlarına şamil edilir.

Qeyd olunan sahənin Azərbaycanda nisbətən yeni olması və mövcud elmi-praktik mənbələrdə sistemli yanaşmanın hələ tam formalaşmaması bu sahədə beynəlxalq təcrübənin öyrənilməsini zəruri edir. Mövcud praktiki çətinliklərin və tənzimləmə boşluqlarının aradan qaldırılması üçün beynəlxalq təcrübə nəzərə alınmaqla monitorinq mexanizmlərinə dair vahid standartların hazırlanması, risk əsaslı istisnaların tətbiqi şərtlərinin dəqiq müəyyən edilməsi və mövcud qaydaların konkretləşdirilməsi vacibdir. Bu məqsədlə məqalədə GMA-nın anlayışı və elementləri, onun tətbiq sahəsi, qanunvericilikdə müəyyən edilmiş istisna hallar, beynəlxalq yanaşmalar və digər əlaqəli məsələlər müzakirə olunur. Bununla yanaşı, ödəniş xidməti təchizatçılarının monitorinq mexanizmlərini necə qurmalı olduqları və bu mexanizmlər vasitəsilə hansı hallarda GMA tələbindən azad edilə biləcəkləri də araşdırılır.

Payments Under GDPR and PSD2: A Case of Cumulative Application, *Privacy and Identity Management* 78 (Michael Friedewald et al. eds., 2021).

[2] Europol, Internet Organised Crime Threat Assessment (IOCTA), 30, § 4.1, Burada bax: https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf (son baxış 13 sentyabr 2026).

[3] Daha ətraflı bax: "Ödəniş xidmətləri və ödəniş sistemləri haqqında" Azərbaycan Respublikasının Qanunu (2023).

[4] Azərbaycan Respublikası Mərkəzi Bankının İdarə Heyətinin 2024-cü il 13 mart tarixli 12/2 nömrəli Qərarı ilə təsdiq edilmiş "Gücləndirilmiş müştəri autentifikasiyasının tətbiqi Qaydası" (2024).

I. GMA-nın elementləri və onların tətbiq xüsusiyyətləri

Elektron ödəniş xidmətlərinin inkişafı və ödəniş əməliyyatlarının məsafədən həyata keçirilməsi imkanlarının genişlənməsi müştərilərin etibarlı şəkildə müəyyənləşdirilməsini və icazəsiz əməliyyatların qarşısının alınmasını xüsusi əhəmiyyətli məsələyə çevirmişdir. Bu baxımdan GMA ödəniş xidmətlərinin təhlükəsizliyinin təmin edilməsinə və ödəniş əməliyyatları zamanı fırıldaqçılıq risklərinin azaldılmasına xidmət edən mühüm mexanizmlərdən biridir.

GMA dedikdə, autentifikasiya məlumatlarının məxfiliyini qorumaq üçün hazırlanmış və yalnız müştərinin və ya müraciət edən fiziki şəxsin "bildiyi", "sahib olduğu" və ya ona "məxsus olan" müstəqil elementlərin iki və ya daha çoxunun istifadəsinə əsaslanan autentifikasiya başa düşülür.[5]

GMA-nın yuxarıda göstərilmiş anlayışından göründüyü kimi onun tətbiqinin əsas məqsədi autentifikasiya məlumatlarının məxfiliyini qorumaqdır. Lakin autentifikasiya prosesində istifadə olunan hər bir məlumat avtomatik olaraq GMA elementi hesab edilmir. GMA çərçivəsində əhəmiyyət kəsb edən məsələ həmin məlumatın autentifikasiya elementi funksiyasını yerinə yetirib-yetirməməsidir. Bu fərq kart rekvizitləri, OTP kodları və digər autentifikasiya vasitələrinin hüquqi qiymətləndirilməsi zamanı xüsusi əhəmiyyət kəsb edir və növbəti hissələrdə ayrıca təhlil olunur.

GMA-nın anlayışına əsasən, başqa adı ilə deyilsə, ikili faktor autentifikasiyasının tətbiqi zamanı azı iki element ("bildiyi", "sahib olduğu", "məxsus olan" element kateqoriyaları) mövcud olmalı və bu iki element eyni kateqoriyaya aid olmamalıdır. Bunun əsas məqsədi isə elementlərin müstəqil mövcudluğunu təmin etməkdir.[6]

Yəni bir elementin pozulmasının digər elementin etibarlılığına xələl gətirməməsi təmin edilməlidir: parol ("bildiyi") və mobil cihaz ("sahib olduğu") kombinasiyası GMA-nın tətbiqinə bir misaldır. Burada elementlər iki fərqli kateqoriyaya məxsusdur və bir elementin oğurlanması digər elementin mövcudluğuna xələl gətirmir. Lakin hər iki autentifikasiya elementi sahib olduğu element kateqoriyasına aid olsabu halda sahib olduğu elementin oğurlanması digər elementin mövcudluğuna xələl gətirə bilər. Belə ki, mobil cihaz və parol müxtəlif kateqoriyalı autentifikasiya elementləri olduğundan mobil cihazın ələ keçirilməsi özlüyündə parolun da əldə edilməsinə səbəb olmaya bilər. Lakin mobil cihaz və OTP-SMS eyni

[5] Anete Boze, Strong Customer Authentification When Providing a Payment Service, *Individual. Society. State. Proceedings of the International Student and Teacher Scientific and Practical Conference* 144, 144 (2021).

[6] European Banking Authority, Single Rulebook Q&A 2020_5619: Independence of the elements for SCA (23 aprel 2021), https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5619 (son baxış 29 sentyabr 2026).

kateqoriyaya aid olduğundan mobil cihazın ələ keçirilməsi həmin şifrənin də üçüncü şəxslər tərəfindən əldə edilməsinə imkan yarada bilər. Qeyd olunan tələbin məqsədi autentifikasiya prosesində yüksək təhlükəsizlik səviyyəsini təmin etməklə yanaşı, istifadəçi təcrübəsinin də qorunmasıdır. Bu baxımdan autentifikasiya müxtəlif texniki üsullarla, o cümlədən istifadəçinin başqa tətbiqə yönləndirilməsi və ya təsdiqləmənin ayrıca cihaz və ya kanal vasitəsilə həyata keçirilməsi formasında təşkil oluna bilər. Bununla belə, seçilən autentifikasiya üsulu istifadəçi üçün lüzumsuz keçidlərə, əlavə təsdiq mərhələlərinə və ya əməliyyatın tamamlanmasını çətinləşdirən digər maneələrə səbəb olmamalıdır. Əks halda, bu cür yanaşma ödəniş əməliyyatlarının icra mexanizminin səmərəliliyini azaldar, istifadəçi təcrübəsini mənfi təsir altına alar və nağdsız hesablaşmaların geniş tətbiqini zəiflədər.

GMA-nın tətbiqinə dair istisnalar və praktiki məsələlərə keçməzdən əvvəl, onun əsasını təşkil edən "bildiyi", "sahib olduğu" və "məxsus olduğu" autentifikasiya elementlərinin hər birinin ayrıca təhlil edilməsi onun mahiyyətinin qavranılması baxımından zəruridir.

A. "Bildiyi" elementi

GMA elementlərindən biri olan "bildiyi" element dedikdə, müştərinin yalnız özünə məlum olan məlumatlar nəzərdə tutulur. Azərbaycan qanunvericiliyində bu elementə dair nümunələr geniş şəkildə təsvir edilməmiş, yalnız "şifrə, PIN, təhlükəsizlik sualları və s." kimi ümumi şəkildə qeyd olunmuşdur.[7] Lakin beynəlxalq yanaşmada hansı məlumatların "bildiyi" element hesab edildiyi və onların GMA tələblərinə uyğunluğu daha geniş formada əks olunmuşdur (Cədvəl 1).[8]

Cədvəl 1-dən göründüyü kimi, istifadəçi adı və ya elektron poçt ünvanı "bildiyi" element kateqoriyasına daxil edilmir. Bunun əsas səbəbi ondan ibarətdir ki, istifadəçi adı və elektron poçt ünvanı yalnız istifadəçiyə məlum olan məlumatlar hesab edilmir, əksinə, onlar üçüncü şəxslər tərəfindən asanlıqla əldə oluna və ümumi informasiya kimi məlum ola bilər.[9] Halbuki daha öncədən qeyd olunduğu kimi, "bildiyi" element yalnız istifadəçiyə məlum olan və məxfiliyi qorunan məlumatı ifadə etməlidir.

[7] Daha ətraflı bax: Azərbaycan Respublikası Maliyyə Monitorinqi Xidmətinin 21 fevral 2023-cü il tarixli, 3-21-28/3-6-4/2023 nömrəli Qərarı ilə təsdiq edilmiş "Müştəri uyğunluğu və yeni texnologiyaların tətbiqi zamanı verifikasiya tədbirlərinə, risk faktorlarının müəyyən edilməsinə və müştəri profilinin risk qruplarına aid edilməsinə dair Qaydalar".

[8] European Banking Authority, Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2, 8, table 3 (2019). Burada bax: https://eba.europa.eu/sites/default/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf (son baxış 28 sentyabr 2026).

[9] Yenə orada, 8, § 34.

"Bildiyi" elementlər çərçivəsində istifadə olunan autentifikasiya vasitələrindən biri suallar toplusudur. Bu autentifikasiya metodunun tətbiqi zamanı xidmət təchizatçıları tərəfindən istifadəçiyə ünvanlanan suallar elə tərtib edilməlidir ki, onların cavabları yalnız istifadəçiyə məlum olsun və məxfi xarakter daşısın, üçüncü şəxslər tərəfindən əldə edilməsi isə mümkün olmasın. Bu kontekstdə bəzi hallarda suallar toplusuna şəxsin doğum tarixi kimi məlumatlar da daxil edilir. Lakin belə məlumatların "bildiyi" element kimi qəbul edilib-edilməməsi mübahisəli xarakter daşıyır. Bunun əsas səbəbi ondan ibarətdir ki, istifadəçi adı və elektron poçt ünvanı kimi doğum tarixi də bir çox hallarda sosial şəbəkələr və digər açıq mənbələr vasitəsilə üçüncü şəxslər tərəfindən əldə oluna bilən məlumatdır. Bu baxımdan doğum tarixi kimi açıq məlumatlar autentifikasiya elementi kimi istifadə üçün uyğun hesab edilmir.[10]

Suallar toplusu kontekstində doğum tarixi ilə yanaşı qeyd edilməlidir ki, müştəridən əməliyyat tarixçəsi, iş yeri və son əməliyyatın həyata keçirildiyi yerlə bağlı verilən suallar da "bildiyi" element hesab edilməməlidir.[11] Çünki sözügedən məlumatlar ödəniş xidməti təchizatçılarının işçiləri və potensial olaraq digər şəxslər tərəfindən asanlıqla əldə edilə bilir.[12] Bununla belə, suallar toplusunun məzmunu yalnız bu cür məlumatlarla məhdudlaşmır və istifadəçiyə elə suallar ünvanlana bilər ki, onların cavabları yalnız istifadəçiyə məlum olsun və üçüncü şəxslər tərəfindən əldə edilməsi mümkün olmasın.

Ümumilikdə suallar toplusu istifadəçilər üçün sadə və əlçatan sayılmasına baxmayaraq, istifadə olunan sualların cavablarının üçüncü şəxslər tərəfindən əldə edilə bilməsi ehtimalı bu autentifikasiya üsulunun əsas zəif tərəflərindən biri kimi qiymətləndirilə bilər. Belə ki, müvafiq məlumatların açıq mənbələr və ya sosial mühəndislik üsulları vasitəsilə əldə edilməsi GMA prosesinin etibarlılığını əhəmiyyətli dərəcədə azalda bilər. Bu səbəbdən suallar toplusunun "bildiyi" elementi kimi etibarlılığı sualların düzgün seçilməsindən və onların cavablarının yalnız istifadəçiyə məlum olmasından asılıdır. Bu şərtlər təmin edildikdə isə suallar toplusu həm istifadəçi, həm də ödəniş xidməti təchizatçısı üçün çevik olması, habelə ayrıca texniki vasitə və ya əlavə resurs tələb etməməsi baxımından əlverişli autentifikasiya vasitəsi hesab edilə bilər.

[10] European Banking Authority, Single Rulebook Q&A 2021_5821: Strong customer authentication (SCA) Knowledge element: Place of Birth and Date of Birth (30 iyun 2021), https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2021_5821 (son baxış 29 sentyabr 2026).

[11] European Banking Authority, Single Rulebook Q&A 2020_5215: Elements of possession (SIM card) and knowledge (knowledge-based responses to challenges or questions) (5 noyabr 2021), https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5215 (son baxış 29 sentyabr 2026).

[12] Yenə orada.

Cədvəl 1. mümkün olan "bildiyi" elementlərin natamam siyahısı

Element kimi	GMA-ya uyğundur?
Parol	Bəli
PIN	Bəli
Suallar toplusu	Bəli
Şifrə ifadəsi	Bəli
Yadda qalan sürüşdürmə yolu[13]	Bəli
Elektron poçt ünvanı və ya istifadəçi adı	Xeyr
Kart məlumatları (kartın üzərində çap olunmuş)	Xeyr
OTP	Xeyr
Çap edilmiş matriks kartı və ya OTP siyahısı	Xeyr

**GMA tələblərinə uyğunluq elementlərin tətbiqində istifadə olunan konkret yanaşmadan asılıdır.*

Beləliklə, "bildiyi" elementin əsas xüsusiyyəti onun yalnız istifadəçiyə məlum olan və məxfiliyi təmin edilən məlumatlara əsaslanmasıdır. Bu baxımdan üçüncü şəxslər tərəfindən asanlıqla əldə edilə bilən və ya açıq mənbələrdə mövcud olan məlumatların autentifikasiya elementi kimi qəbul edilməsi GMA-nın mahiyyətinə uyğun hesab edilmir. Nəticə etibarilə, "bildiyi" elementin effektivliyi və etibarlılığı birbaşa olaraq həmin məlumatın məxfilik səviyyəsindən və istifadəçi ilə məhdud əlaqələndirilməsindən asılıdır.

B. "Sahiblik" elementi

GMA-nın növbəti elementi isə "sahiblik" elementidir. Adından da göründüyü kimi, "sahiblik" elementi istifadəçinin yalnız öz nəzarətində olan və ona məxsus fiziki və ya rəqəmsal vasitəyə əsaslanan autentifikasiya faktorunu ifadə edir. Bu element yalnız istifadəçinin fiziki olaraq sahib olduğu vasitələri deyil, həmçinin fiziki mülkiyyətində olmasa da, onun istifadəsində və nəzarətində olan elementləri də əhatə edir.[14] Buna misal olaraq istifadəçinin mobil telefonuna yüklənmiş tətbiqləri göstərmək olar. Bu baxımdan "sahiblik" elementi öz mahiyyətinə görə istifadəçi ilə konkret bir vasitə arasında davamlı əlaqənin mövcudluğunu tələb edir və həmin vasitənin autentifikasiya prosesində identifikasiyaedici rol oynamasını təmin edir.

"Sahiblik" elementi ilə əlaqədar bir sıra sual doğuran məqamlar vardır. Bunlardan biri SMS vasitəsilə alınan OTP kodların və şifrələrin hansı səbəbdən fərqli autentifikasiya elementlərinə aid edilməsidir. İlkin baxışda hər iki məlumat oxşar görünür, çünki həm şifrə, həm də OTP kod müəyyən hərf və ya rəqəmlərdən ibarətdir. Lakin OTP kodların mahiyyəti təhlil

[13] Yadda qalan sürüşdürmə yolu - İstifadəçinin mobil cihaz və ya sistemə giriş üçün ekranda müəyyən istiqamətlərdə sürüşdürmə hərəkətləri ilə yaratdığı unikal qrafik şifrələmə üsulu.
[14] Yuxarıda istinad 8, 6, § 24.

edildikdə aydın olur ki, autentifikasiya baxımından əsas əhəmiyyət kəsb edən kodun özü deyil, həmin kodun göndərildiyi və istifadəçinin nəzarəti altında olan SIM kart və ya mobil cihazdır. Başqa sözlə, SMS vasitəsilə göndərilən OTP kodu "sahiblik" elementinin mövcudluğunu təsdiq edən vasitə kimi çıxış edir. Məhz bu səbəbdən SMS OTP mexanizmi "sahiblik" elementinə aid edilir. Digər tərəfdən, hesaba təyin edilən şifrə hər hansı konkret cihaza bağlı olmur və istifadəçinin özü tərəfindən müəyyən edilərək yadda saxlanılır. Buna görə də şifrə "bildiyi" elementə aid edilir.

Digər bir məsələ isə kart rekvizitlərinin, yəni kart nömrəsinin, etibarlılıq müddətinin və CVV kodunun GMA çərçivəsində hansı hüquqi statusa malik olması, başqa sözlə, onların "bildiyi" elementə, "sahiblik" elementinə aid edilməsi və ya ümumiyyətlə autentifikasiya elementi hesab olunub-olunmamasıdır. İlk baxışda "bildiyi" element kimi görünsə də, bu rekvizitlər kartın üzərində açıq şəkildə əks olunur. GMA çərçivəsində "autentifikasiya məlumatının məxfiliyinin qorunması" prinsipi əsas götürüldükdə, aydın olur ki, bu cür məlumatlar nə "bildiyi", nə də "sahiblik" elementi kimi qiymətləndirilə bilər. Belə ki, autentifikasiya elementləri öz təbiətinə görə məxfiliyin təmin olunmasına xidmət etməlidir. Kart rekvizitlərinin kartın üzərində açıq şəkildə göstərilməsi isə onların məxfiliyini azaldır, beləliklə həmin məlumatların autentifikasiya elementi kimi qəbul olunmasını şübhə altına alır.

Bununla belə, statik CVV kodunun GMA çərçivəsində autentifikasiya elementi hesab edilməməsi onun təhlükəsizlik baxımından əhəmiyyət kəsb etmədiyi anlamına gəlmir. CVV kodu ilkin olaraq kartın həqiqiliyinin yoxlanılması və ödəniş əməliyyatı zamanı istifadə olunan kart məlumatlarının müəyyən mərhələdə fiziki kartdan əldə edildiyini təsdiq etmək məqsədilə yaradılmışdır.[15] Başqa sözlə, bu kodun funksiyası GMA çərçivəsində "sahiblik" elementini təmin etmək deyil, kart məlumatlarının etibarlılığının yoxlanılmasına xidmət edən əlavə təhlükəsizlik vasitəsi kimi çıxış etməkdir. Məhz bu səbəbdən statik CVV kodunun məxfiliyinin qorunması vacib olsa da, onun kart üzərində açıq şəkildə əks olunması GMA baxımından həmin kodun müstəqil autentifikasiya elementi kimi qəbul edilməsinə imkan vermir.

Statik CVV kodunun müstəqil autentifikasiya elementi olmadığını müəyyən edildikdən sonra kart nömrəsi və etibarlılıq müddəti kimi digər rekvizitlərin hüquqi statusu ayrıca təhlil olunmalıdır. Həmin rekvizitlər arasında ilk olaraq kart nömrəsinin hüquqi statusuna nəzər salmaq məqsədəuyğundur. Kart nömrəsi kart üzərində göstərilməsə belə, onun "sahiblik" elementi kimi qəbul edilməsi məqsədəuyğun hesab edilmir. Belə ki, kart nömrəsi istifadəçinin konkret karta və ya cihaza nəzarət etdiyini öz-

[15] Ramon Degennaro, *Merchant Acquirers and Payment Card Processors: A Look Inside the Black Box*, 91 Federal Reserve Bank of Atlanta Economic Review 27, 40 (2006).

özlüyündə təsdiqləmir. Bundan əlavə, kart nömrəsi müəyyən əməliyyatlar zamanı üçüncü şəxslərə təqdim oluna bilir. Bu səbəbdən o, yalnız istifadəçinin nəzarətində olan autentifikasiya vasitəsi kimi qiymətləndirilə bilməz. Etibarlılıq müddəti də mahiyyət etibarilə müstəqil autentifikasiya funksiyası yerinə yetirməyən və yalnız kartın texniki rekvizitlərindən birini təşkil edən statik məlumat olduğundan, onun da autentifikasiya elementi kimi qəbul edilməsi əsaslı hesab edilmir.

Kart nömrəsi və etibarlılıq müddətindən fərqli olaraq, CVV kodu yalnız müəyyən şərtlər daxilində "sahiblik" elementi kimi qiymətləndirilə bilər. Bu həmin kodun kartın üzərində açıq şəkildə əks olunmadığı və təhlükəsizlik məqsədləri üçün dinamik şəkildə dəyişən xarakter daşıdığı hallara aiddir.[16] Əks halda, yəni CVV kodunun kart üzərində sabit formada göstərilməsi onun da məxfilik xüsusiyyətini zəiflədir və nəticə etibarilə autentifikasiya elementi kimi qəbulunu məhdudlaşdırır.

Eyni yanaşma digər oxşar hallara da şamil edilir. EBA-nın mövqeyinə əsasən, kart rekvizitləri kimi əvvəlcədən çap olunmuş OTP siyahıları da autentifikasiya elementi hesab edilmir. Belə ki, bu kodların üçüncü şəxslər tərəfindən əldə edilməsi riski onların məxfiliyinin təmin olunmasını çətinləşdirir. Bunun əksinə olaraq, fiziki formada mövcud olan kartın özü "sahiblik" elementi kimi çıxış edir. Bu, xüsusilə bankomatlardan nağd pul çıxarılması zamanı GMA-nın tətbiqində özünü aydın şəkildə göstərir. Belə ki, bu halda autentifikasiya iki müstəqil elementin kombinasiyası əsasında həyata keçirilir: istifadəçinin bildiyi PIN kodu və onun nəzarətində olan fiziki ödəniş kartı.[17]

Müasir dövrdə kartın sahibliyi yalnız fiziki forma ilə məhdudlaşmır, rəqəmsal mühitdə də reallaşa bilər. Buna nümunə olaraq Apple Pay rəqəmsal ödəniş alətini göstərmək olar. Bu sistemdə ödəniş kartı rəqəmsal cüzdana əlavə edilərkən emitent tərəfindən kartın etibarlılığı yoxlanılır, kart məlumatları isə cihaz üçün unikal ödəniş tokeni ilə əvəz edilərək təhlükəsiz mühitdə saxlanılır.[18] Beləliklə, istifadəçinin həmin etibarlı cihaz üzərində nəzarəti autentifikasiya prosesində "sahiblik" elementinin rəqəmsal təzahürü kimi çıxış edir.

Rəqəmsal ödəniş mühitində "sahiblik" elementi təkcə rəqəmsal cüzdanda saxlanılan ödəniş kartı ilə məhdudlaşmır. Bu baxımdan istifadəçinin mobil

[16] Yuxarıda istinad 8, 6, § 25; EBA, Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC, 7, § 35 (2018). Burada bax: https://www.eba.europa.eu/sites/default/files/documents/10180/2137845/0f525dc7-0f97-4be7-9ad7-800723365b8e/Opinion%20on%20the%20implementation%20of%20the%20RTS%20on%20SCA%20and%20CSC%20(EBA-2018-Op-04).pdf?retry=1 (son baxış 29 sentyabr 2026).

[17] Yuxarıda istinad 4, bənd 2.4.

[18] Apple Inc., Payment authorization with Apple Pay, https://support.apple.com/en-az/guide/security/secc1f57e189/web (son baxış 28 sentyabr 2026).

cihazı və həmin cihaz üzərində istifadə olunan mobil tətbiq də "sahiblik" elementi kimi çıxış edə bilər. Bununla belə, eyni hesabın bir neçə mobil cihazda istifadə edilməsi hallarında konkret cihazın "sahiblik" elementi kimi qiymətləndirilməsi müəyyən hüquqi və texniki məsələlər yaradır. Əgər konkret mobil cihaz ödəniş xidməti təchizatçısı tərəfindən GMA çərçivəsində etibarlı cihaz kimi tanınır və istifadəçi ilə əlaqələndirilirsə, həmin cihaz sonrakı autentifikasiya proseslərində "sahiblik" elementi kimi qəbul edilə bilər.

Mobil cihazlarla yanaşı, digər texnoloji həllər də müəyyən şərtlər daxilində "sahiblik" elementinin təmin edilməsinə xidmət edə bilər. Bu baxımdan QR kodlardan istifadə "sahiblik" elementinin tətbiqinə dair nümunələrdən biri hesab olunur. Belə ki, müəyyən hallarda QR kod ödəniş xidməti istifadəçisinin ödəniş alətinə və ya ödəniş hesabına nəzarət etdiyini təsdiq edən vasitə kimi çıxış edə bilər.[19] Bu, məsələn, istifadəçinin ödəniş hesabında yaradılmış QR kodun təqdim edilməsi və ya ödəniş xidməti istifadəçisinə məxsus etibarlı cihaz vasitəsilə QR kodun skan edilməsi yolu ilə həyata keçirilə bilər.

Cədvəl 2. Mümkün olan "sahiblik" elementlərinin natamam siyahısı[20]

Element kimi	**GMA-ya uyğundur?**
OTP ilə təsdiqlənən Cihazın mövcudluğu (aparat və ya proqram token generatoru, SMS OTP)	Bəli
Cihazın mövcudluğu cihaz tərəfindən yaradılmış rəqəmsal imza ilə təsdiqlənir	Bəli
QR kod və ya foto TAN vasitəsilə kart və ya cihazın mövcudluğu təsdiqlənir	Bəli
Tətbiq və ya brauzer cihazla bağlanmışdır (təhlükəsizlik çipi, xüsusi açar, brauzerin qeydiyyatı ilə)	Bəli
Kartın mövcudluğu kart oxuyucu vasitəsilə	Bəli
Kartın dinamik təhlükəsizlik kodu ilə təsdiqi	Bəli
Cihaza yüklənmiş tətbiq	Xeyr
Kart üzərində yazılmış məlumatlar (kart nömrəsi, CVV)	Xeyr
Çap edilmiş element (məsələn, OTP siyahısı)	Xeyr

[19] Yuxarıda istinad 8, 6, § 27.

[20] Yuxarıda istinad 8, 7, table 2.

**GMA tələblərinə uyğunluq, elementlərin tətbiqində istifadə olunan konkret yanaşmadan asılıdır.*

"Sahiblik" elementinin müxtəlif formalarının təhlilindən sonra bu elementin daha müasir və geniş tətbiq olunan formalarından biri kimi ani bildirişlərə (push notifications) ayrıca nəzər yetirmək məqsədəuyğundur. Ani bildiriş ödəniş xidməti təchizatçısı tərəfindən xidmət istifadəçisinə məxsus olan mobil cihazına və ya mobil tətbiqinə göndərilən autentifikasiya vasitəsidir.[21] Bu mexanizm çərçivəsində istifadəçiyə təqdim olunan təsdiq bildirişi ödəniş əməliyyatı ilə dinamik şəkildə əlaqələndirilmiş element kimi çıxış edir və praktikada OTP kod əsaslı təsdiq üsullarının alternativ forması kimi istifadə olunur. Hər iki mexanizmin ümumi xüsusiyyəti ondan ibarətdir ki, autentifikasiya məlumatı konkret ödəniş əməliyyatı ilə dinamik şəkildə əlaqələndirilir.

Ani bildirişlərin tətbiqi ilə bağlı digər mühüm məsələ onların GMA-nın hansı elementinə aid edilməsinin müəyyən edilməsidir. Ümumiyyətlə, ani bildirişin göndərildiyi mobil cihaz "sahiblik" elementi kimi qiymətləndirilsə də, bildirişin təsdiqlənməsi üsulundan asılı olaraq autentifikasiya prosesində əlavə olaraq "bildiyi" və ya biometriya elementlərindən də istifadə oluna bilər. Ani bildirişlərin təsdiqi zamanı cihazın kilidini açmaq üçün biometrik məlumatdan ("məxsusluq" elementi) və ya PIN kodu daxil etməkdən ("bildiyi" elementi) istifadə olunması mexanizmi iki fərqli kateqoriyaya aid elementi birləşdirdiyi üçün GMA tələbini ödəmiş olur.

Yuxarıda qeyd olunanlardan göründüyü kimi, mobil cihazlar müxtəlif autentifikasiya mexanizmləri çərçivəsində "sahiblik" elementi kimi çıxış edə bilər. Bununla belə, mobil cihazdan istifadə edilməsi və ya onun vasitəsilə autentifikasiyanın həyata keçirilməsi həmin mexanizmin bütün hallarda GMA tələblərinə uyğun olması demək deyildir. Bu məsələ xüsusilə ödəniş kartlarının elektron cüzdanlara əlavə edilməsi və tokenləşdirilməsi prosesində əhəmiyyət kəsb edir. Belə ki, həmin proseslərdə istifadə olunan autentifikasiya vasitələrinin GMA elementi kimi qiymətləndirilməsi onların yalnız texniki xüsusiyyətlərindən deyil, həm də ödəniş xidməti təchizatçısının autentifikasiya prosesindəki rolundan və müvafiq təhlükəsizlik mexanizmləri ilə əlaqəsindən asılıdır.

Rəqəmsal ödəniş xidmətlərinin genişlənməsi nəticəsində ödəniş kartlarının elektron cüzdanlara əlavə edilməsi və tokenləşmə mexanizmlərinin tətbiqi ödəniş təhlükəsizliyinin təminində əsas məsələlərdən birinə çevrilmişdir. Bu proses zamanı GMA tətbiqi tələbi xüsusilə vacibdir. Belə ki, ödəniş xidməti təchizatçıları uzaq kanallar

[21] European Banking Authority, Single Rulebook Q&A 2019_4984: "Push based" authentication and SCA requirements (25 sentyabr 2020), https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2019_4984 (son baxış 29 sentyabr 2026).

vasitəsilə aparılan və ödəniş fırıldağı və ya digər sui-istifadə riski daşıyan hər bir əməliyyat zamanı GMA tətbiq etməlidirlər.[22] Bu tələblərin praktiki icrası isə Apple Pay və Google Pay kimi texniki xidmət təchizatçılarının ödəniş kartlarının elektron cüzdanlara əlavə edilməsi və tokenləşdirilməsi prosesindəki rolu ilə birbaşa bağlıdır.

Apple Pay və ya Google Pay "Ödəniş xidmətləri və ödəniş sistemləri haqqında" Qanunun 3.2.13-cü bəndində qeyd edilmiş ödəniş xidmətlərinin göstərilməsini dəstəkləmək məqsədilə texniki xidmət təchizatçıları olaraq köçürmə prosesinin hər hansı anında köçürülən vəsaitlərə sahiblik etmədən təqdim olunan xidmətləri[23] həyata keçirir.[24] Bu xidmətlər ödəniş kartlarının tokenləşdirilməsini və autentifikasiya üçün zəruri texniki infrastrukturun təmin edilməsini əhatə etsə də, ödəniş əməliyyatının emalı və avtorizasiyası müvafiq ödəniş infrastrukturu çərçivəsində ekvayer, kart şəbəkəsi və emitent tərəfindən həyata keçirilir.

Kredit institutları tərəfindən müzakirə olunan məsələlərdən biri də ödəniş kartlarının müxtəlif elektron cüzdanlara əlavə edilməsi zamanı istifadə olunan autentifikasiya vasitələrinin GMA elementləri çərçivəsində hansı statusa malik olmasıdır. Belə ki, kartın elektron cüzdana əlavə edilməsi prosesində istifadəçi mobil cihazın kilidini barmaq izi, üz tanınma və ya parol vasitəsilə açа bilər. İlk baxışda bu vasitələr müvafiq olaraq "məxsusluq" və ya "bildiyi" elementlər kimi görünə bilər. Lakin bu cür autentifikasiya vasitələrinin mövcudluğu özlüyündə onların GMA elementi kimi qəbul edilməsi üçün kifayət etmir. Bunun əsas səbəbi ondan ibarətdir ki, həmin biometrik məlumatlar və ya parollar adətən mobil cihazın əməliyyat sistemi səviyyəsində idarə olunur və ödəniş əməliyyatını həyata keçirən ödəniş xidməti təchizatçısının təhlükəsizlik infrastrukturu ilə birbaşa əlaqələndirilmir.[25] Başqa sözlə, bu autentifikasiya vasitələri ödəniş xidməti təchizatçısı tərəfindən yaradılmır, idarə olunmur və onun nəzarəti altında olmur.

Buna görə də istifadəçinin mobil cihazını açmaq üçün tətbiq etdiyi barmaq izi, üz tanınma və ya parol kartın elektron cüzdana əlavə edilməsi

[22] European Commission, Directive No. 2015/2366, art. 97 (2015).

[23] Bu xidmətlərə məlumatların emalı, saxlanması, autentifikasiyası, təhlükəsizliyinin təmin edilməsi, o cümlədən, ödəniş xidmətlərinin təminatında istifadə olunan informasiya texnologiyaları, rabitə şəbəkəsi, habelə texniki cihazların təchizatı və dəstəklənməsi daxildir.

[24] European Banking Authority, Single Rulebook Q&A 2021_6141: Association of personalised security credentials to the payment service user (17 dekabr 2021), https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2021_6141 (son baxış 29 sentyabr 2026).

[25] European Banking Authority, Single Rulebook Q&A 2021_6145: SCA applicability / Application of SCA at tokenisation stage (31 yanvar 2023), https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2021_6145 (son baxış 29 sentyabr 2026).

kontekstində avtomatik olaraq GMA elementi hesab edilmir. Bu vasitələrin GMA çərçivəsində nəzərə alınması üçün onların ödəniş xidməti təchizatçısının autentifikasiya mexanizmləri ilə etibarlı şəkildə əlaqələndirilməsi və autentifikasiya prosesinin bir hissəsi kimi istifadə olunması tələb olunur.

Beləliklə, "sahiblik" elementi müxtəlif formalarda, fiziki kartlardan tutmuş mobil cihazlar, rəqəmsal pul kisələri və QR kodlar kimi texnoloji vasitələrə qədər, özünü göstərə bilər. Lakin bütün bu hallarda əsas meyar dəyişməz qalır: müvafiq vasitə yalnız istifadəçinin nəzarətində olmalı və autentifikasiya prosesində onun identifikasiyasına xidmət etməlidir. Bu xüsusiyyətlərin təmin olunmadığı hallarda isə həmin vasitənin "sahiblik" elementi kimi qiymətləndirilməsi mümkün olmur.

C. "Məxsusluq" elementi

GMA-nın əsas elementlərindən biri də "məxsusluq" elementidir. "Məxsusluq" elementi istifadəçinin özünəməxsus fiziki, fizioloji və ya davranış xüsusiyyətlərinə əsaslanan autentifikasiya faktorunu ifadə edir. Digər autentifikasiya elementlərindən fərqli olaraq, bu element istifadəçinin malik olduğu vasitələrə və ya bildiyi məlumatlara deyil, onun şəxsiyyəti ilə ayrılmaz şəkildə bağlı olan xüsusiyyətlərə əsaslanır.

"Məxsusluq" elementi çərçivəsində istifadə olunan autentifikasiya vasitələrinə barmaq izi, damar nümunəsi, üz həndəsəsi, əl həndəsəsi, səs nümunəsi, retina və ya göz bəbəyi skanı kimi biometrik göstəricilər aid edilə bilər.[26] Müasir texnologiyaların inkişafı nəticəsində "məxsusluq" elementi artıq yalnız ənənəvi biometrik göstəricilərlə məhdudlaşmır. Belə ki, istifadəçinin yazı yazma üslubu, klaviaturadan istifadə davranışı və digər davranış biometrikaları da müəyyən hallarda "məxsusluq" elementi kimi istifadə edilə bilər.

Bununla belə, hər bir biometrik göstəricinin avtomatik olaraq GMA-nın "məxsusluq" elementi hesab edilməsi mümkün deyildir.[27] Bu qiymətləndirmə biometrik göstəricinin özündən deyil, onun tətbiq olunduğu autentifikasiya həllinin GMA tələblərinə uyğunluğundan asılıdır. Bu baxımdan biometrik məlumatın təhlükəsiz şəkildə saxlanılması və emal edilməsi, kifayət qədər etibarlı identifikasiya təmin etməsi, eləcə də digər autentifikasiya elementlərindən müstəqilliyinin qorunması əsas meyarlar hesab olunur. Aşağıdakı cədvəldə biometrik və digər "məxsusluq" elementlərinin tam olmayan siyahısı və onların GMA kontekstində qiymətləndirilməsi təqdim edilmişdir.

[26] Boze, yuxarıda istinad 5, 146; yuxarıda istinad 8, 5.

[27] Yenə orada.

Cədvəl 3. Mümkün olan "məxsusluq" elementlərinin natamam siyahısı[28]

Element kimi	GMA-ya uyğundur?
Barmaq izi skanı	Bəli
Səs tanınması	Bəli
Damar tanınması	Bəli
Əl və üz geometriyası	Bəli
Retina və iris skanı[29]	Bəli
Klaviatura vuruş dinamikası	Bəli
Ürək döyüntüsü və ya digər bədən hərəkəti nümunələri, istifadəçinin şəxs olduğunu müəyyən etmək üçün (məsələn, geyinilə bilən cihazlarda)	Bəli
Cihazın tutulma bucağı	Bəli
EMV® 3-D Secure kimi kommunikasiya protokolu vasitəsilə ötürülən məlumat	Xeyr (hazırda bazarda müşahidə olunan yanaşmalar üçün)
Yadda saxlanılan sürüşdürmə yolu	Xeyr

**GMA tələblərinə uyğunluq, elementlərin tətbiqində istifadə olunan konkret yanaşmadan asılıdır.*

D. Elementlərin müstəqilliyi prinsipi

GMA-nın əsas xüsusiyyətlərindən biri autentifikasiya elementlərinin bir-birindən müstəqil olmasıdır. Elementlərin müstəqilliyi GMA-nın fundamental prinsiplərindən biri olmaqla, autentifikasiya elementlərindən birinin məxfiliyinin pozulmasının digər elementin təhlükəsizliyinə təsir göstərməməsini ifadə edir. Başqa sözlə, autentifikasiya elementləri elə təşkil edilməlidir ki, onlardan birinin ələ keçirilməsi və ya təhlükəsizliyinin pozulması digər elementin etibarlılığını və təhlükəsizliyini zəiflətməsin. Bu yanaşma GMA-nın təhlükəsizlik məqsədinin həyata keçirilməsində mühüm rol oynayır və çoxfaktorlu autentifikasiyanın etibarlılığını təmin edir.

Azərbaycan Respublikasının qanunvericiliyində də bu prinsip öz əksini tapmışdır. Belə ki, elementlərin müstəqilliyi dedikdə, bir elementin ələ

[28] Yuxarıda istinad 8, 5, table 1.

[29] Retina və iris skanı - insanın göz quruluşuna əsaslanan biometrik identifikasiya üsulu olub, iris və retina səviyyəsindəki unikal naxışların rəqəmsal analizini həyata keçirir. Bu texnologiya şəxsiyyətin dəqiq və etibarlı tanınmasını təmin edən göz biometrik sistemlərindən biridir.

keçirilməsi halının digər elementin təhlükəsizliyinə xələl gətirməməsi nəzərdə tutulur. Milli qanunvericilik bu prinsipi autentifikasiya elementlərinin təhlükəsizliyinin qorunmasına yönəlmiş əsas tələblərdən biri kimi müəyyən etmişdir.[30]

Bununla belə, RTS elementlərin müstəqilliyi prinsipini Azərbaycan Respublikasının qanunvericiliyindən daha ətraflı şəkildə tənzimləmişdir. RTS yalnız autentifikasiya elementlərindən birinin məxfiliyinin pozulmasının digər elementə təsir göstərməməsi tələbi ilə kifayətlənmir, eyni zamanda bu prinsipin praktik tətbiqi zamanı yarana biləcək texniki riskləri də nəzərə alaraq onların azaldılmasına yönəlmiş əlavə təhlükəsizlik tələbləri müəyyən edir.[31] Bu baxımdan RTS-nin 9-cu maddəsi xüsusi əhəmiyyət kəsb edir. Həmin maddənin 2-ci bəndinə əsasən, GMA elementlərinin çoxfunksiyalı cihaz vasitəsilə istifadəsi əlavə təhlükəsizlik riskləri yaradır, çünki belə cihazlar zərərli proqramların və ya haker müdaxiləsinin hədəfinə çevrilə bilər. Məsələn, müştərinin smartfon vasitəsilə həm birdəfəlik parolu SMS-lə alması, həm də ödəniş əməliyyatını həmin cihazda təsdiqləməsi bu riskə nümunədir. Belə risklərin azaldılması üçün ödəniş xidməti təchizatçısı əlavə təhlükəsizlik tədbirləri görməlidir. Bu tədbirlərdən biri autentifikasiyanın TEE (Trusted execution environment) adlı qorunan sahədə yerinə yetirilməsidir. Bu yanaşmanın tətbiqinə Apple Pay[32] və Google Pay[33] kimi mobil ödəniş vasitələrini nümunə göstərmək olar. Bu sistemlərdə kart məlumatlarının və autentifikasiya ilə bağlı əməliyyatların qorunması üçün cihazın yaddaşından deyil, çiplərindən istifadə edilir.

Beləliklə, elementlərin müstəqilliyi prinsipi yalnız autentifikasiya zamanı müxtəlif kateqoriyalı elementlərdən istifadə edilməsini deyil, həm də həmin elementlərin təhlükəsizliyinin bir-birindən asılı olmamasını tələb edir. Bu baxımdan autentifikasiya elementlərinin eyni cihaz vasitəsilə tətbiqi özlüyündə müstəqillik prinsipinin pozulması kimi qiymətləndirilməməli, əsas diqqət həmin cihazın təhlükəsizliyinin pozulmasının digər autentifikasiya elementinin etibarlılığına təsir edib-etməməsinə yönəldilməlidir. Buna görə də GMA-nın effektivliyi autentifikasiya elementlərinin düzgün seçilməsi ilə yanaşı, onların tətbiqi zamanı müstəqilliyin texniki və təşkilati tədbirlərlə təmin olunmasından da asılıdır.

[30] Yuxarıda istinad 7, mad. 7.1.3.

[31] European Commission, Regulation No. 2018/389, art. 9 (2018).

[32] Apple Inc., Apple Pay Security and Privacy Overview, https://support.apple.com/en-us/101554 (son baxış 28 sentyabr 2026).

[33] Google LLC, Google Pay Safety & Security Features, https://safety.google/intl/en/products/pay/ (son baxış 28 sentyabr 2026).

II. GMA-nın tətbiqində istisna hallar: milli qanunvericilik və beynəlxalq yanaşma

A. Azərbaycan Respublikasının GMA Qaydasına əsasən istisnalar

GMA ödəniş əməliyyatlarının təhlükəsizliyinin təmin edilməsində əsas mexanizmlərdən biri olsa da, onun tətbiqi bütün hallarda məcburi xarakter daşımır. Qanunvericilikdə müəyyən əməliyyatlar və situasiyalar üzrə risk əsaslı yanaşmanı rəhbər tutaraq GMA-nın tətbiqindən istisnalar nəzərdə tutulur. Belə ki, Qaydalar bir tərəfdən ödəniş əməliyyatlarının təhlükəsizliyini qorumaq, digər tərəfdən isə aşağı riskli əməliyyatlar zamanı istifadəçilər üçün əlavə əməliyyat yükünün və narahatlığın qarşısını almaq məqsədi daşıyır.

Qaydada nəzərdə tutulmuş istisnaları aşağıdakı şəkildə bir neçə qrupa bölmək olar:

- istifadəçinin statusu ilə bağlı istisnalar,
- ödəniş əməliyyatının xüsusiyyətindən irəli gələn istisnalar,
- sessiya və autentifikasiya prosesinə aid istisnalar,
- hesab məlumatlarına çıxışla bağlı istisnalar,
- risk əsaslı yanaşmaya əsaslanan istisnalar.

İstifadəçinin statusu ilə bağlı istisnalar. Qaydanın 3.11-ci bəndinə əsasən, hüquqi şəxslər üçün yaradılan və təhlükəsizlik üzrə xüsusi ödəniş kanalları vasitəsilə aparılan ödənişlər zamanı GMA tətbiq edilməyə bilər. Bu müddəadan göründüyü kimi, Qayda fiziki şəxslər üçün nəzərdə tutulan yanaşmadan fərqli olaraq, hüquqi şəxslər tərəfindən həyata keçirilən ödəniş əməliyyatları üçün ayrıca tənzimləmə mexanizmi müəyyən etmişdir.[34] Burada "xüsusi ödəniş kanalları" dedikdə yalnız hüquqi şəxslər üçün əlçatan olan, yüksək təhlükəsizlik səviyyəsini təmin edən və səlahiyyətli orqan tərəfindən GMA ilə ən azı ekvivalent təhlükəsizlik təmin etdiyi qəbul edilən xüsusi ödəniş prosesləri və ya protokollar nəzərdə tutulur. Bu cür kanallara korporativ host-to-host inteqrasiyaları, API əsaslı korporativ ödəniş həlləri və ya SWIFT kimi xüsusi korporativ ödəniş şəbəkələri aid edilə bilər.[35]

Sessiya və autentifikasiya prosesi ilə bağlı istisnalar. İlk növbədə qeyd edilməlidir ki, ödəniş alətlərinin mobil tətbiqlərə və ya digər proqram təminatlarına əlavə edilməsi zamanı GMA-nın tətbiqi tələb olunmur. Lakin yenə də belə hallarda ən azı autentifikasiya həyata keçirilməlidir.[36] Bunun əsas səbəbi ondan ibarətdir ki, ödəniş alətinin mobil tətbiqə əlavə edilməsi

[34] Yuxarıda istinad 4, bənd 3.11.

[35] European Banking Authority, Single Rulebook Q&A 2018_4383: Exemption of secure corporate payment processes and protocols (26 fevral 2021), https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2018_4383 (son baxış 29 sentyabr 2026).

[36] Yuxarıda istinad 4, bənd 3.13.

özlüyündə ödəniş əməliyyatının icrası ilə nəticələnmir və vəsaitin köçürülməsinə səbəb olmur. Lakin həmin ödəniş aləti sonradan maliyyə əməliyyatlarının həyata keçirilməsi üçün istifadə ediləcəyindən, onun yalnız hüquq sahibi tərəfindən əlavə edilməsinin təmin edilməsi məqsədilə istifadəçinin ən azı autentifikasiya olunması tələb edilir.[37] Qaydalardan fərqli olaraq, Avropa İttifaqı hüququnda kartın rəqəmsal cüzdana əlavə edilməsi dələduzluq riski yaradan hərəkət kimi qiymətləndirildiyindən, PSD2 çərçivəsində bu mərhələdə GMA-nın tətbiq edilməsi tələb olunur.[38]

Sessiya və autentifikasiya prosesi ilə bağlı digər mühüm istisna istifadəçinin artıq GMA-dan keçdiyi hallarda eyni sessiya çərçivəsində həmin autentifikasiyanın təkrar tətbiq edilməsinin tələb olunmamasıdır. Belə ki, əgər ödəniş hesabına daxil olmaq üçün GMA tətbiq edilirsə, bu sessiya çərçivəsində GMA tələb edən əməliyyat apardıqda bu əməliyyat GMA tətbiq edilmədən aparıla bilər.[39] Lakin bu hal autentifikasiya tətbiqini istisna etmir. Eyni sessiyanın hüdudları istifadəçinin fəaliyyət göstərmədiyi halda sessiyanın nə qədər aktiv saxlanıla biləcəyinə dair müəyyən edilmiş müddətlərlə müəyyən olunur.[40] Mobil tətbiqlərdə bu müddət 5 (beş) dəqiqə, internet bankçılığında isə 30 (otuz) dəqiqədir. Bu müddətlər başa çatdıqdan sonra sessiya yeni sessiya hesab edilir və GMA-nın yenidən tətbiq edilməsi zərurəti yarana bilər.[41] Qaydanın bu bəndində "hər hansı fəaliyyət" anlayışına normativ tərifin verilməməsi həmin müddəanın tətbiqində qeyri-müəyyənliklər yarada bilər. Lakin bu qeyri-müəyyənliklərin aydınlaşdırılması üçün EBA-nın izahlarına nəzər yetirmək olar. Belə ki, EBA-nın izahlarında bu anlayış istifadəçinin sessiya çərçivəsində hesab məlumatlarına baxması, ödəniş təşəbbüsü göstərməsi, məlumat daxil etməsi və ya digər aktiv əməliyyatları həyata keçirməsi kimi təqdim edilmişdir.[42] İstifadəçi tərəfindən ən azı qeyd edilən hərəkətlərin edilmədən açıq saxlanılması isə "fəaliyyətsizlik" kimi qiymətləndirilir və bu halda müəyyən edilmiş müddət başa çatdıqdan sonra sessiya dayandırılmalıdır.

Hesab məlumatlarına çıxışla bağlı istisnalar. Qanunvericilik müəyyən hallarda istifadəçinin hesab məlumatlarına GMA tətbiq edilmədən çıxışına

[37] Yenə orada.

[38] EBA clarifies the application of strong customer authentication requirements to digital wallets, European Banking Authority (31 yanvar 2023), https://www.eba.europa.eu/publications-and-media/press-releases/eba-clarifies-application-strong-customer-authentication (son baxış 29 sentyabr 2026).

[39] Yuxarıda istinad 4, bənd 3.4.

[40] Yenə orada, yarımbənd 2.2.5.

[41] Yenə orada.

[42] European Banking Authority, Single Rulebook Q&A 2018_4068: Exemption from strong customer authentication (SCA) for payment account information in combination with accessing account information online in web browser (21 dekabr 2018), https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2018_4068 (son baxış 29 avqust 2026).

icazə verir. Bu istisnanın əsas məqsədi istifadəçi rahatlığının təmin edilməsi olmaqla yanaşı, aşağı riskli hesab olunan məlumat sorğularında təkrar GMA tətbiqinin qarşısını almaqdır. Belə ki, istifadəçi ödəniş hesabının balansına dair məlumat əldə etdikdə və ya ödəniş hesabı üzrə son 180 gün ərzində həyata keçirilmiş ödəniş əməliyyatlarına dair məlumatları əldə etdikdə, həmin məlumatlara GMA tətbiq edilmədən çıxış əldə edə bilər.[43]

Bununla belə, bu istisna mütləq xarakter daşımır. Qayda üç halda GMA-nın yenidən tətbiqini tələb edir. Birincisi, ödəniş xidməti istifadəçisi həmin məlumatlara məsafədən ilk dəfə çıxış əldə etdikdə. İkincisi, istifadəçi son 180 gün ərzində ödəniş əməliyyatlarının tarixçəsini əldə etmək məqsədilə ödəniş hesabına son GMA tətbiqindən sonra 180 gündən artıq müddət keçdikdə. Üçüncüsü isə müştərinin həssas ödəniş məlumatlarının açıqlanması hallarında.

Müştərinin həssas məlumatları anlayışı, "Ödəniş xidmətləri və ödəniş sistemləri haqqında" Qanunda təsbit olunmuşdur. Bura fırıldaqçılıq əməliyyatının aparılması üçün istifadə edilə bilən, fərdiləşdirilmiş təhlükəsizlik məlumatlarının da daxil olduğu məlumatlar aid edilir. Bununla belə, bu Qanunda həssas ödəniş məlumatları anlayışına münasibətdə istisna da müəyyən edilmişdir. Belə ki, ödəniş əməliyyatlarının aparılması üçün vasitəçilik xidməti və hesab üzrə məlumat xidməti göstərilən hallarda istifadəçinin adı və hesab nömrəsi barədə məlumatlar həssas ödəniş məlumatları hesab edilmir.[44]

Qanunda məhz ödəniş əməliyyatlarının aparılması üçün vasitəçilik xidməti və hesab üzrə məlumat xidməti ilə bağlı xüsusi istisnanın nəzərdə tutulması həmin xidmətlərin ayrıca nəzərdən keçirilməsini zəruri edir. Bu xidmətlər açıq bankçılıq modelinin əsas elementlərindən hesab olunduğundan, Avropa İttifaqı qanunvericiliyində onlara münasibətdə ayrıca tənzimləmə mexanizmi formalaşdırılmışdır. Belə ki, 2018-ci ildə qəbul edilmiş RTS-yə 2022-ci ildə edilmiş dəyişikliklərlə, xüsusilə AISP-lərin (hesab üzrə məlumat xidməti göstərən xidmət təchizatçısı) fəaliyyətinə dair yeni tələblər müəyyən edilmişdir.[45] Həmin dəyişikliklər banklardan fərqli olaraq bu xidmət təchizatçılarının məlumatlara çıxışı, autentifikasiya prosesində iştirakı və məlumatların idarə edilməsi ilə bağlı əlavə qaydaları əhatə edir. Belə ki, 2022-ci ildə RTS-yə edilmiş dəyişikliklərlə hesab məlumatlarına birbaşa ödəniş hesabına xidmət göstərən ödəniş xidməti təchizatçısı vasitəsilə çıxış və AISP vasitəsilə çıxış halları fərqləndirilmiş, AISP vasitəsilə çıxış zamanı GMA-nın tətbiqindən istisna ayrıca tənzimlənmişdir. Azərbaycan

[43] Yuxarıda istinad 4, bənd 3.1.

[44] Yuxarıda istinad 3, mad. 1.1.23 (bu Qanunun 3.1.6-cı və 3.1.7-ci maddələrində nəzərdə tutulan ödəniş xidmətlərinin göstərilməsi zamanı ödəniş xidməti istifadəçisinin adı və hesab nömrəsi haqqında məlumat istisna olmaqla).

[45] European Commission, Regulation 2022/2360, art. 1(2) (2022) (RTS-ə əlavə edilmiş maddə 10a ilə bağlı).

Respublikasının qanunvericiliyində isə hazırda PISP (Payment initiation service provider) və AISP-lərin fəaliyyəti ilə bağlı ayrıca və ətraflı GMA-ya dair tənzimləmə mexanizmi nəzərdə tutulmamışdır. Bu istisnaların mahiyyətinin və GMA-nın tətbiqində yaratdığı xüsusiyyətlərin daha aydın anlaşılması üçün AISP və PISP-lərin ödəniş prosesində yerinə yetirdiyi funksiyaların ayrıca nəzərdən keçirilməsi məqsədəuyğundur.

AISP-lər açıq bankçılıq ekosistemində fəaliyyətin əsas iştirakçılarından biridir. Onlar müştərinin icazəsi ilə bank hesab məlumatlarını əldə edərək emal edir və müxtəlif maliyyə xidmətlərinin göstərilməsinə şərait yaradırlar.[46] PISP isə AISP-dən fərqli olaraq ödəniş təşəbbüsü xidmətləri təqdim edir. Yəni bu təchizatçı müştərinin adından birbaşa onun bank hesabı vasitəsilə ödəniş əməliyyatlarını başladır. RTS-də qeyd edilən əsas məqamlardan biri də ondan ibarətdir ki, ASPSP-lər (Account Servicing Payment Service Provider) (xüsusən banklar) PISP və AISP-lərin fəaliyyətinə autentifikasiya prosesləri zamanı böyük maneələr yaratmamalıdırlar.[47] Bu tələbin məqsədi, açıq bankçılıq ekosistemində rəqabətin və innovasiyaların təşviq olunması, həmçinin xidmətlərə maneəsiz və təhlükəsiz çıxışın təmin edilməsidir.

Yuxarıda qeyd edilmiş hesaba çıxışla bağlı istisnalarda xüsusi qeyd edilməli məqamlardan biri RTS-də edilmiş dəyişiklikdir. Belə ki, RTS-nin əvvəlki formasında[48] 10-cu maddədə qeyd olunmuşdur ki, "ödəniş xidməti təchizatçısı aşağıdakı məlumatlardan birini və ya hər ikisini", yəni həm balans məlumatını, həm də son 90 gün ərzində həyata keçirilən əməliyyat tarixcəsini GMA tətbiq etmədən istifadəçiyə göstərə bilər.[49] Lakin yeni dəyişikliyə əsasən bu müddəada sözügedən anlayış "aşağıdakı məlumatlardan birini" ifadəsi ilə əvəzlənmişdir. Bu dəyişikliklə bağlı aydınlaşdırılması zəruri olan əsas məsələ ondan ibarətdir ki, yeni redaksiya GMA-nın tətbiqindən istisnanın eyni vaxtda yalnız bir məlumat növünə şamil edilməsini nəzərdə tutur, yoxsa hesabın balansı və əməliyyat tarixçəsi barədə məlumatların hər ikisinə eyni vaxtda GMA tətbiq edilmədən çıxış imkanını saxlayır. Bu dəyişikliklə 10 və 10a nömrəli maddələrində "biri və ya hər ikisi" ifadəsi "biri" ifadəsi ilə əvəz olunsa da, EBA qeyd etmişdir ki, bu dəyişiklik 90 günlük istisnanın mahiyyətini dəyişdirmir. EBA-nın izahına əsasən,[50] GMA-nın tətbiq edilmədiyi hallar həm hesab qalığına, həm də son 90 gün ərzində həyata keçirilmiş əməliyyatların tarixçəsinə çıxışı əhatə etməyə

[46] Michał Grabowski, *Account Information and Payment Initiation Services and the Related AML Obligations in the Law of the European Union*, 3 FinTech 173, 178 (2024).

[47] European Banking Authority, Single Rulebook Q&A 2023_6767: App to app redirection with biometrics for PIS (29 sentyabr 2023), https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2023_6767 (son baxış 29 avqust 2026).

[48] Yuxarıda istinad 31.

[49] European Banking Authority, Single Rulebook Q&A 2023_6820: Exemption from strong customer authentication (29 sentyabr 2023), https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2023_6820 (son baxış 29 avqust 2026).

[50] Yenə orada.

davam edir, o şərtlə ki, həssas ödəniş məlumatları açıqlanmasın və digər tələblərə riayət olunsun. 2022/2360 saylı Qərarın 4-cü əsaslandırma bəndində də bu mövqe təsdiqlənir və orada açıq şəkildə "hesab qalığına və son əməliyyatlara çıxış" ifadəsinə yer verilir.[51] Buna görə də bu dəyişiklik maddənin tətbiq sahəsini məhdudlaşdıran deyil, yalnız redaksiya xarakterli düzəliş kimi qiymətləndirilməlidir. Lakin Qaydada açıq şəkildə qeyd olunmuşdur ki, bu əməliyyatların hər ikisi GMA-sız həyata keçirilə bilər.

Ödəniş əməliyyatının xüsusiyyətindən irəli gələn istisnalar. Bu istisnalardan biri təmassız ödəniş əməliyyatları ilə bağlıdır. Təmassız ödəniş əməliyyatı dedikdə, kart məlumatlarının təmassız texnologiyalar vasitəsilə radiotezliklərlə ötürülməsi ilə həyata keçirilən ödəniş əməliyyatı nəzərdə tutulur. Təmassız ödənişlər zamanı bir ödənişin məbləği 100 manatdan, bu cür əməliyyatların günlük həcmi isə 500 manatdan çox olduqda GMA tətbiq edilməlidir.[52] RTS-də isə bu fərqli məbləğlərlə tənzimlənir. Belə ki, GMA tətbiq edilmədən həyata keçirilən təmassız ödəniş əməliyyatının yuxarı həddi 50 Euro olaraq müəyyənləşdirilmişdir. Axırıncı dəfə GMA tətbiq edilməklə həyata keçirilən ödəniş əməliyyatından sonra GMA-sız tətbiq edilən ödəniş əməliyyatların cəmi məbləği 150 Euro-dan çox olmamalıdır və bu əməliyyatların sayı isə 5-i keçməməlidir.[53] Bu istisnanın əsas məqsədi aşağı riskli və kiçik məbləğli gündəlik ödənişlərin daha sürətli həyata keçirilməsini təmin etməklə yanaşı, istifadəçi rahatlığını artırmaqdır. Bununla belə, EBA vurğulayır ki, təmassız ödənişlərə münasibətdə nəzərdə tutulmuş bu istisna mütləq xarakter daşımır.[54] Ödəniş xidməti təchizatçısı fırıldaqçılıq riskinin artdığını müəyyən etdikdə və ya öz risk idarəetmə siyasəti çərçivəsində zəruri hesab etdikdə, qanunvericilikdə müəyyən edilmiş hədlərə çatılmasa da, GMA-nın tətbiq edilməsini tələb edə bilər.[55] Bu yanaşma istisnanın istifadəçi rahatlığının təmin edilməsinə xidmət etməsi ilə yanaşı, təhlükəsizlik tələblərinin də daim qorunmasına yönəldiyini göstərir.

Ödəniş əməliyyatının xüsusiyyətindən irəli gələn digər istisna etibar edilən şəxslər siyahısı və dövri ödənişlərlə bağlıdır. Bu siyahılara daxil edilmiş ödənişlər GMA tətbiq edilmədən həyata keçirilə bilər. Lakin siyahıların ilk dəfə tərtib edilməsi və ya mövcud siyahılara dəyişiklik edilməsi zamanı GMA tətbiq olunmalıdır.[56]

---

[51] Yenə orada; yuxarıda istinad 45, 4-cü əsaslandırma bəndi.

[52] Yuxarıda istinad 4, bənd 3.5.

[53] Yuxarıda istinad 31, 4.

[54] European Banking Authority, Single Rulebook Q&A 2018_4225: Contactless payments at point of sale - Applications of the conditions (11 oktyabr 2019), https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2018_4225 (son baxış 29 avqust 2026).

[55] Yuxarıda istinad 45, art.4.

[56] Yuxarıda istinad 4, bənd 3.6, 3.7.

GMA Qaydası qəbul edilməzdən əvvəl yaradılmış dövri ödənişlərə münasibətdə GMA-nın tətbiqi məsələsi də xüsusi diqqət tələb edir. EBA-nın yanaşmasına əsasən, belə ödənişlər üzrə GMA-nın yenidən tətbiq edilməsi tələb olunmur. Lakin dövri ödənişin şərtlərində dəyişiklik edildiyi halda, həmin dəyişiklik yeni razılıq tələb edən hal kimi qiymətləndirildiyindən GMA-nın tətbiqi zəruri hesab edilir.[57]

Etibar edilən şəxslər siyahısı ilə bağlı mübahisə doğuran məsələlərdən biri ödəniş xidməti istifadəçisinin ödəniş əməliyyatını təsdiq etmək üçün tətbiq etdiyi GMA proseduru çərçivəsində eyni zamanda vəsait alanı da etibar edilən şəxslər siyahısına əlavə etməsinin mümkün olub-olmamasıdır. RTS-nin 13-cü maddəsi etibar edilən şəxslər siyahısına daxil edilmiş vəsait alanlara edilən ödənişlər üzrə GMA istisnasını nəzərdə tutsa da, həmin maddənin tətbiqinə dair EBA-nın mövqeyinə əsasən, ödəniş xidməti istifadəçisi müəyyən şərtlər daxilində ödəniş əməliyyatını təsdiq etdiyi eyni GMA proseduru vasitəsilə vəsait alanı etibar edilən şəxslər siyahısına da əlavə edə bilər.[58] Bunun üçün istifadə olunan autentifikasiya mexanizmi həm konkret ödəniş əməliyyatının məbləği, həm də vəsait alan ilə dinamik şəkildə əlaqələndirilməlidir.

Azərbaycan Respublikasının GMA Qaydasında isə bu məsələyə dair ayrıca tənzimləmə nəzərdə tutulmamışdır. Bununla belə, autentifikasiya elementinin əməliyyatın məbləği və vəsait alan ilə dinamik şəkildə əlaqələndirilməsi prinsipi əks olunmuşdur.[59] Lakin həmin norma eyni GMA proseduru çərçivəsində həm ödəniş əməliyyatının təsdiq edilməsi, həm də vəsait alanın etibar edilən şəxslər siyahısına əlavə olunmasının mümkünlüyünü ayrıca tənzimləmir. Bu baxımdan EBA-nın yanaşması milli qanunvericilikdə nəzərdə tutulmuş ümumi dinamik əlaqələndirmə prinsipini konkretləşdirən və onun praktik tətbiqini izah edən mühüm hüquqi mövqe kimi qiymətləndirilə bilər.

Ödəniş əməliyyatının xüsusiyyətindən irəli gələn növbəti istisna eyni ödəniş xidməti təchizatçısında açılmış ödəniş hesabları arasında həyata keçirilən kredit köçürmələri ilə bağlıdır. Belə ki, ödəniş xidməti istifadəçisinin eyni ödəniş xidməti təchizatçısında xidmət olunan ödəniş hesabları arasında həyata keçirdiyi kredit köçürmələri zamanı GMA tətbiq edilməyə bilər.[60]

[57] European Banking Authority, Single Rulebook Q&A 2018_4048: Applicability of Strong Customer Authentication (SCA) to existing recurring payments solutions (14 dekabr 2018), https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2018_4048 (son baxış 29 avqust 2026).

[58] European Banking Authority, Single Rulebook Q&A 2023_6827: Trusted Beneficiaries (29 sentyabr 2023), https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2023_6827 (son baxış 29 avqust 2026).

[59] Yuxarıda istinad 4, bənd 2.3.

[60] Yenə orada, bənd 3.8.

Kredit köçürməsi dedikdə isə, ödəniş hesabına xidmət göstərən ödəniş xidməti təchizatçısı tərəfindən vəsaitin köçürülməsi məqsədilə ödəyicinin ödəniş sərəncamı əsasında icra edilən ödəniş aləti başa düşülür.[61]

Məsələn, istifadəçinin eyni bankda açılmış cari hesabından əmanət hesabına və ya digər şəxsi hesabına vəsait köçürməsi istisna çərçivəsində qiymətləndirilə bilər.[62] Bunun əsas səbəbi ondan ibarətdir ki, həm göndərən, həm də qəbul edən hesablar eyni ödəniş xidməti təchizatçısı tərəfindən idarə olunur və əməliyyatın risk səviyyəsi digər kredit köçürmələri ilə müqayisədə daha aşağı hesab edilir. Bununla belə, bu istisna ödəniş xidməti təchizatçısının risk əsaslı qiymətləndirmə aparmaq və zəruri hallarda GMA tətbiq etmək səlahiyyətini istisna etmir. Beləliklə, sözügedən istisna təhlükəsizlik tələblərinin zəiflədilməsi deyil, aşağı riskli əməliyyatlar üzrə istifadəçi rahatlığının təmin edilməsinə xidmət edir.

Bir digər istisna isə aşağı məbləğli və məsafədən həyata keçirilən elektron ödəniş əməliyyatları ilə bağlıdır. Bu istisna ardıcıl şəkildə həyata keçirilən aşağı riskli əməliyyatlarda hər bir ödəniş üzrə GMA-nın təkrar tətbiq edilməsinin qarşısını almağa xidmət edir. Belə ki, sonuncu GMA tətbiq edilməklə həyata keçirilmiş ödəniş əməliyyatından sonra ardıcıl olaraq həyata keçirilən məsafədən elektron ödəniş əməliyyatlarının sayı beşdən və ya onların ümumi məbləği 300 manat və ya ekvivalentindən çox olmadıqda, məbləği 60 manat və ya ekvivalentindən çox olmayan ödəniş əməliyyatı GMA tətbiq edilmədən həyata keçirilə bilər.[63]

Məsələn, ödəyici sonuncu dəfə GMA tətbiq edilməklə 100 manat məbləğində ödəniş əməliyyatı həyata keçirmişdir. Bundan sonra o, ardıcıl olaraq 20 manat, 50 manat, 40 manat, 40 manat və 60 manat məbləğində olmaqla beş məsafədən elektron ödəniş əməliyyatı həyata keçirərsə, həmin əməliyyatların hər birinin məbləği 60 manatdan, ümumi məbləği isə 300 manatdan artıq olmadığından GMA-nın yenidən tətbiqi tələb olunmur. Lakin altıncı ödəniş əməliyyatı həyata keçirilərkən, məbləğindən asılı olmayaraq, ardıcıl əməliyyatların sayı beşi keçdiyi üçün GMA-nın yenidən tətbiq edilməsi zəruri olur. Bu hal aşağıdakı cədvəldə əyani şəkildə göstərilmişdir:

Cədvəl 4. İstisna halın tətbiq forması

Ödəniş sayı	**Ödəniş məbləği**	**GMA tələb olunur?**
1-ci	20 AZN	Xeyr
2-ci	50 AZN	Xeyr
3-cü	40 AZN	Xeyr
4-cü	40 AZN	Xeyr
5-ci	60 AZN	Xeyr

[61] Yuxarıda istinad 3, mad. 1.2.26.

[62] Yuxarıda istinad 4, bənd 3.8.

[63] Yenə orada, bənd 3.9.

6-cı	10 AZN	**Bəli** – çünki 5-dən artıqdır.

Eyni qayda, ardıcıl həyata keçirilən ödəniş əməliyyatlarından hər hansı birinin məbləği 60 manatı aşdığı hallara da şamil edilmir. Belə ki, sonuncu dəfə GMA tətbiq edilməklə həyata keçirilmiş ödəniş əməliyyatından sonra həyata keçirilən ödənişlərdən hər hansı birinin məbləği 60 manatdan çox olduqda, həmin ödəniş əməliyyatına münasibətdə müvafiq istisna tətbiq edilmir və GMA-nın tətbiqi tələb olunur.

Risk əsaslı istisnalar. Qaydanın 3.10-cu bəndinə əsasən, ödəniş xidməti təchizatçısı tərəfindən bu Qaydanın 4.2-ci bəndinin şərtləri gözlənilməklə aşağı riskli hesab olunan ödəniş əməliyyatları GMA tətbiq edilmədən aparıla bilər.[64] Aşağı riskli ödəniş əməliyyatlarının müəyyən edilməsi meyarları və bu istisnanın tətbiqi şərtləri növbəti paraqrafda təhlil ediləcəkdir.

Qaydada nəzərdə tutulmuş istisna halların təhlilini tamamlayarkən keçid xarakterli tənzimləmə nəzərdə tutan 3.12-ci bəndə də ayrıca toxunmaq zəruridir. Həmin bəndə əsasən, 1 yanvar 2026-cı il tarixinədək elektron ticarət çərçivəsində həyata keçirilən ödəniş əməliyyatları GMA tətbiq edilmədən icra edilə bilərdi. Elektron ticarət dedikdə, informasiya sistemlərindən istifadə etməklə malların alqı-satqısı, xidmətlərin göstərilməsi və işlərin görülməsi ilə bağlı həyata keçirilən fəaliyyət başa düşülür. Qaydanın 3.13-cü bəndi həmin keçid dövründə belə əməliyyatların tamamilə təhlükəsizlik tədbirlərindən azad edilməsini nəzərdə tutmurdu. Belə ki, qeyd olunan tarixədək elektron ticarət əməliyyatlarının ən azı autentifikasiyadan keçirilməsi tələb olunurdu.

Yuxarıda nəzərdən keçirilən istisnalarla yanaşı, GMA-nın tətbiqi baxımından hüquqi qiymətləndirilməsi xüsusi əhəmiyyət kəsb edən digər hallar da mövcuddur. Bunlardan biri ödəniş əməliyyatının məsafədən deyil, ödəniş xidməti təchizatçısının xidmət göstərdiyi məkanda istifadəçinin fiziki iştirakı ilə, lakin elektron vasitələrdən istifadə edilməklə həyata keçirilməsidir. Bu baxımdan belə bir sual yaranır: ödəniş xidməti istifadəçisi bank filialına şəxsən müraciət etdikdə və kredit köçürməsi üzrə ödəniş tapşırığı bank əməkdaşının təqdim etdiyi elektron cihaz vasitəsilə formalaşdırıldıqda, həmin əməliyyatın başlanılması zamanı GMA-nın tətbiqi tələb olunurmu? Bu məsələnin qiymətləndirilməsi zamanı aşağıdakı sualların cavablandırılması əhəmiyyət kəsb edir:

-ilk növbədə, belə əməliyyatın ümumiyyətlə GMA Qaydasının tətbiq dairəsinə daxil olub-olmaması;

-əgər GMA Qaydası tətbiq olunarsa, bank əməkdaşı tərəfindən həyata keçirilən fiziki identifikasiyanın GMA çərçivəsində elektron autentifikasiyanı əvəz edib-etməməsi;

[64] Yenə orada, bənd 3.10.

-nəhayət, belə əməliyyatın risk səviyyəsi nəzərə alınmaqla onun aşağı riskli əməliyyat kimi qiymətləndirilərək GMA-dan azad edilməsinin mümkün olub-olmaması.

İlk növbədə qeyd edilməlidir ki, PSD2-nin 95-ci əsaslandırma hissəsində (Recital 95) elektron formada təqdim edilən ödəniş xidmətlərinin təhlükəsiz autentifikasiya mexanizmləri vasitəsilə həyata keçirilməsinin zəruriliyi vurğulansa da, kağız daşıyıcılarında, poçt və ya telefon vasitəsilə verilən ödəniş sərəncamlarının eyni autentifikasiya tələblərinə tabe tutulmasının zəruri olmadığı qeyd edilmişdir. Bu yanaşmanı inkişaf etdirən digər bir EBA yanaşmasına əsasən, ödəniş xidməti istifadəçisi bank filialında şəxsən iştirak etdikdə və ödəniş tapşırığı bank əməkdaşının təqdim etdiyi elektron cihaz vasitəsilə qəbul edildikdə, belə əməliyyat PSD2-nin 97-ci maddəsinin 1-ci bəndinin (b) yarımbəndi mənasında ödəyicinin elektron ödəniş əməliyyatını başlaması kimi qiymətləndirilmir.[65] Bundan əlavə, PSD2-nin 4-cü maddəsinin 29-cu bəndinə əsasən, autentifikasiya dedikdə, ödəniş xidməti təchizatçısına ödəniş xidməti istifadəçisinin şəxsiyyətini və ya konkret ödəniş alətindən istifadə hüququnu yoxlamağa imkan verən prosedur başa düşülür. Bu baxımdan ödəniş xidməti istifadəçisi ödəniş xidməti təchizatçısının filialına şəxsən müraciət etdikdə və onun şəxsiyyəti birbaşa təchizatçının əməkdaşı tərəfindən müəyyən edildikdə, istifadəçinin identifikasiyası elektron mühitdə həyata keçirilən autentifikasiya prosesindən mahiyyət etibarilə fərqlənir.[66] Bu səbəblərdən həmin hallarda GMA-nın tətbiqindən söhbət getmir.

İkinci məsələyə gəldikdə isə, belə hallarda istifadəçinin şəxsiyyəti elektron autentifikasiya elementləri vasitəsilə deyil, ödəniş xidməti təchizatçısının əməkdaşı tərəfindən fiziki identifikasiya yolu ilə müəyyən edilir. Bu baxımdan bank əməkdaşı tərəfindən həyata keçirilən fiziki identifikasiya GMA çərçivəsində autentifikasiya elementlərini əvəz edən mexanizm deyil, istifadəçinin şəxsiyyətinin birbaşa müəyyən edilməsinə əsaslanan ayrıca identifikasiya proseduru kimi çıxış edir. Buna görə də istifadəçinin bank filialında fiziki iştirakı və ya şəxsiyyət vəsiqəsini təqdim etməsi GMA-nın "məxsusluq" və ya "sahiblik" elementləri kimi qiymətləndirilmir.

Nəhayət, sözügedən əməliyyatların GMA tələbinin tətbiq dairəsinə daxil olmadığı nəzərə alındıqda, onların aşağı riskli əməliyyat kimi qiymətləndirilərək GMA istisnaları çərçivəsində ayrıca təhlil edilməsinə ehtiyac qalmır. Çünki bu halda söhbət GMA-dan istisnanın tətbiqindən deyil, GMA öhdəliyinin ümumiyyətlə yaranmadığı bir əməliyyatdan gedir.

Yuxarıda qeyd edilən bank filialındakı fiziki iştirak məsələsinin hüquqi həlli üçün bilavasitə Avropa İttifaqı təcrübəsinə müraciət edilməsi milli qanunvericilikdə tənzimləmə boşluqlarının mövcudluğunu göstərir. Məhz bu

[65] European Banking Authority, Single Rulebook Q&A 2020_5124: Trusted Beneficiaries (21 yanvar 2022), https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5124 (son baxış 29 avqust 2026).

[66] Yenə orada.

səbəbdən, Azərbaycan Respublikasının GMA Qaydasında birbaşa öz əksini tapmayan, lakin beynəlxalq praktikada əməliyyat səmərəliliyi üçün geniş tətbiq edilən digər mühüm istisnaların ayrıca nəzərdən keçirilməsi zəruridir.

B. RTS-də nəzərdə tutulan əlavə istisnalar: Azərbaycan qanunvericiliyi ilə müqayisəli təhlil

RTS-də GMA-nın tətbiqindən azad edilən əlavə hallar ödəniş əməliyyatının başlanma üsulu və texniki xüsusiyyətləri nəzərə alınmaqla müəyyən edilmişdir. Bu istisnalar aşağı riskli əməliyyatlarda təhlükəsizlik tələblərini qorumaqla yanaşı, ödəniş prosesinin səmərəliliyini təmin etməyə xidmət edir.

Belə istisnalardan biri elektron poçt vasitəsilə verilən ödəniş tapşırıqları ilə bağlıdır. EBA-nın yanaşmasına[67] əsasən, bu növ əməliyyatlar GMA-nın tətbiq dairəsinə daxil edilmir. Bunun əsas səbəbi ondan ibarətdir ki, bu halda ödəniş əməliyyatı elektron vasitə ilə birbaşa ödəniş xidməti istifadəçisi tərəfindən deyil, onun göstərişi əsasında ödəniş xidməti təchizatçısının əməkdaşı tərəfindən sistemdə başladılır. Bu baxımdan belə əməliyyatlar PSD2-nin 97-ci maddəsinin 1-ci bəndinin (b) yarımbəndində nəzərdə tutulan "ödəyicinin elektron ödəniş əməliyyatını başlaması" anlayışına aid edilmir. Azərbaycan Respublikasının GMA ilə bağlı müvafiq tənzimləmələrində isə elektron poçt vasitəsilə verilən ödəniş tapşırıqlarına münasibətdə analoji istisna ayrıca nəzərdə tutulmamışdır. Bu baxımdan Avropa İttifaqı tənzimləməsindən fərqli olaraq, milli qanunvericilikdə bu növ əməliyyatların GMA-nın tətbiq dairəsindən kənarda qalmasını birbaşa müəyyən edən xüsusi müddəa mövcud deyildir.[68]

RTS-də nəzərdə tutulan digər mühüm istisnalardan biri vəsait alan tərəfindən başladılan ödəniş əməliyyatlarıdır (*Merchant Initiated Transactions – MIT*). EBA-nın yanaşmasına əsasən, bu cür əməliyyatlarda ödəniş konkret əməliyyat anında ödəyici tərəfindən elektron vasitə ilə başlanılmadığından, PSD2-nin 97-ci maddəsində nəzərdə tutulan GMA tələbi tətbiq edilmir.[69] Bununla belə, belə əməliyyatın hüquqi əsasını ödəyicinin əvvəlcədən verdiyi razılıq təşkil etməlidir.

Azərbaycan Respublikasının tənzimləmə sisteminə nəzər yetirdikdə isə bu məsələyə münasibətdə müəyyən fərqlilik müşahidə olunur. Belə ki, PSD2-nin

[67] European Banking Authority, Single Rulebook Q&A 2021_6315: Transactions initiated via electronic mail (email) (6 yanvar 2023), https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2021_6315 (son baxış 29 avqust 2026).

[68] Yuxarıda istinad 4, bənd 3.

[69] EBA, Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC, 7, §§ 45-48 (2018). Burada bax: https://www.eba.europa.eu/sites/default/files/documents/10180/2137845/0f525dc7-0f97-4be7-9ad7-800723365b8e/Opinion%20on%20the%20implementation%20of%20the%20RTS%20on%20SCA%20and%20CSC%20(EBA-2018-Op-04).pdf?retry=1 (son baxış 29 sentyabr 2026).

97-ci maddəsinin 1-ci bəndinin (b) yarımbəndi ilə oxşarlıq təşkil edən "Ödəniş xidmətləri və ödəniş sistemləri haqqında" Azərbaycan Respublikası Qanununun 35.1.2-ci maddəsində GMA-nın tətbiqi ödəyicinin elektron ödəniş əməliyyatını başlatması ilə deyil, elektron ödəniş əməliyyatının aparılması ilə əlaqələndirilmişdir. Bu terminoloji fərq vəsait alan tərəfindən başladılan ödəniş əməliyyatlarının Azərbaycan qanunvericiliyi çərçivəsində GMA-nın tətbiq dairəsinə daxil olub-olmaması məsələsində müəyyən qeyri-müəyyənlik yaradır. Başqa sözlə, mövcud normativ mətn bu cür əməliyyatların Aİ tənzimləməsində olduğu kimi GMA-nın tətbiq dairəsindən kənarda qalmasını, yaxud elektron ödəniş əməliyyatı kimi GMA tətbiq edilməli hallar sırasına daxil olmasını birmənalı şəkildə müəyyən etməyə imkan vermir.

Bununla yanaşı, Azərbaycan Respublikasının mövcud tənzimləmələrində dövri ödənişlər və etibar edilən şəxslər siyahısı üzrə GMA-nın tətbiqindən müəyyən istisnalar nəzərdə tutulsa da,[70] bu istisnalarla vəsait alan tərəfindən başladılan əməliyyatlar arasındakı münasibət ayrıca tənzimlənmir. Bu səbəbdən, təcrübədə ticarət müəssisəsi tərəfindən başladılan müəyyən əməliyyatlara GMA-nın tətbiq edilməməsinin həmin istisnalar çərçivəsində qiymətləndirilməsi mümkün olsa da, bunu MIT-in Azərbaycan qanunvericiliyində ayrıca və ümumi şəkildə GMA-nın tətbiq dairəsindən çıxarılması kimi qiymətləndirmək üçün normativ əsas kifayət qədər aydın deyildir.

Cədvəl 5. İstisnanın tətbiqinə dair xülasə cədvəli [71]

			Vəsait alanın xidmət təchizatçısı	
RTS maddəsi	**İstisnalar**	**Ödəyicinin xidmət təchizatçısı**	**Kredit köçürməsi**	**Kartlar**
Maddə 10	Ödəniş hesabı məlumatlarına çıxış	Bəli	Tətbiq olunmur	Tətbiq olunmur
Maddə 11	POS-da kontaktsız ödənişlər	Bəli	Xeyr	Bəli
Maddə 12	Nəqliyyat və park üçün ödəniş terminalları	Bəli	Xeyr	Bəli
Maddə 13	Etibarlı benefisiarlar	Bəli	Xeyr	Xeyr
Maddə 14	Təkrarlanan əməliyyatlar	Bəli	Xeyr	Bəli

[70] Yuxarıda istinad 4, bənd 3.6.

[71] Yuxarıda istinad 8, 9, table 2.

Maddə 15	Öz hesabına köçürmələr	Bəli	Xeyr	Tətbiq olunmur
Maddə 16	Aşağı məbləğli əməliyyatlar	Bəli	Xeyr	Bəli
Maddə 17	Təhlükəsiz korporativ ödəniş prosesləri və protokollar	Bəli	Xeyr	Tətbiq olunmur
Maddə 18	Əməliyyat risk analizinə əsaslanan istisna	Bəli	Xeyr	Bəli

**Ödəyicinin ödəniş xidməti təchizatçısı (PSP) istənilən halda əməliyyat üzrə GMA-nın tətbiqi barədə yekun qərar verən tərəfdir. Xidmət təchizatçısı texniki imkan olduqda istisnadan imtina edərək GMA-nı tətbiq edə və ya əməliyyatı rədd edə bilər.*

5-ci Cədvəldən çıxan əsas nəticələrdən biri RTS-də GMA istisnalarının tətbiqinin yalnız əməliyyatın növündən deyil, həm də müvafiq ödəniş xidməti təchizatçısının (ödəyicinin və vəsait alanın ödəniş xidməti təchizatçısı) əməliyyatda yerinə yetirdiyi funksiyadan asılı olmasıdır. Bununla yanaşı, müəyyən istisnaların mövcudluğu GMA-nın mütləq tətbiq edilməyəcəyi demək deyildir, çünki yekun qərar hər bir konkret əməliyyat üzrə ödəyicinin ödəniş xidməti təchizatçısı tərəfindən qəbul edilir. Azərbaycan Respublikasının GMA Qaydasında da RTS-də nəzərdə tutulan bir sıra istisnalara mahiyyət etibarilə oxşar hallar müəyyən edilmişdir.[72] Bununla belə, RTS-dən fərqli olaraq, GMA Qaydasında istisnaların tətbiqi ödəyicinin və vəsait alanın ödəniş xidməti təchizatçılarının funksiyaları və ayrı-ayrı ödəniş alətləri üzrə bu şəkildə fərqləndirilmir. Bu baxımdan RTS istisnaların tətbiq mexanizmini və ayrı-ayrı ödəniş xidməti təchizatçılarının bu prosesdəki rolunu daha detallı şəkildə müəyyən edir.

Göründüyü kimi, RTS-də nəzərdə tutulmuş istisnalar da Azərbaycan qanunvericiliyində olduğu kimi, təhlükəsizlik və istifadəçi rahatlığı arasında tarazlığın qorunması məqsədinə xidmət edir. Lakin bu istisnaların tətbiqi ödəniş xidməti təchizatçısını təhlükəsizlik öhdəliklərindən azad etmir. Əksinə, EBA və Avropa Mərkəzi Bankının yanaşmasına uyğun olaraq, GMA-nın tətbiq edilmədiyi hallarda belə, ödəniş xidməti təchizatçısı əməliyyatın risk səviyyəsini davamlı qiymətləndirməli, istifadəçinin davranış modelini, əməliyyatın texniki xüsusiyyətlərini və digər risk indikatorlarını monitorinq etməlidir.[73] Məhz bu yanaşma risk əsaslı autentifikasiya modelinin mahiyyətini təşkil edir və GMA istisnalarının təhlükəsizlik tələblərini zəiflətmədən tətbiq edilməsinə imkan yaradır.

[72]Yuxarıda istinad 4, bənd 3.1, 3.4, 3.9.

[73] Yuxarıda istinad 8, §§ 40-46.

III. Monitorinq mexanizmi necə tənzimlənməli və aşağı riskli əməliyyatlar hansılardır?

GMA-nın əsas məqsədi ödəniş əməliyyatlarının təhlükəsizliyini təmin etmək və qeyri-qanuni müdaxilə riskini minimuma endirməkdir. Bununla belə, GMA-nın bütün ödəniş əməliyyatlarına istisnasız tətbiqi əməliyyatların icra müddətinin artmasına, istifadəçi təcrübəsinin pisləşməsinə və ödəniş xidməti təchizatçıları üçün əlavə inzibati və texniki yükün yaranmasına səbəb ola bilər. Bu səbəbdən qanunvericilik təhlükəsizlik ilə əməliyyat səmərəliliyi arasında balansın qorunması məqsədilə risk əsaslı yanaşmanı qəbul etmişdir.

Həmin yanaşmaya uyğun olaraq, ödəniş xidməti təchizatçıları ödəniş əməliyyatlarını qanunvericilikdə müəyyən edilmiş meyarlar əsasında davamlı monitorinq etməli və yalnız aşağı riskli hesab edilən əməliyyatlara münasibətdə GMA-nın tətbiq edilməməsi imkanından istifadə edə bilərlər. Bu baxımdan monitorinq mexanizmi GMA istisnalarının tətbiqinin əsas hüquqi və texniki təminatlarından biri kimi çıxış edir.

Qayda əməliyyatın aşağı riskli hesab edilmə şərtlərini müəyyənləşdirmişdir. Belə ki, bu əməliyyatlar ilkin olaraq əməliyyatın məbləğindən və fırıldaqçılıq göstəricisindən asılıdır.[74] Bundan əlavə, qanunvericilik risk qiymətləndirilməsinin kompleks yanaşma əsasında həyata keçirilməsini tələb edir.[75] Bu yanaşmaya əsasən, ödəniş xidməti təchizatçısı hər bir əməliyyatı həm statistik göstəricilər, həm də konkret əməliyyatın xüsusiyyətləri baxımından qiymətləndirməlidir. Başqa sözlə, aşağı riskli əməliyyatın müəyyən edilməsi yalnız əvvəlki fırıldaqçılıq göstəricilərinin normativ hədlər daxilində olması ilə məhdudlaşmır. Bunun üçün həm statistik meyarların, həm də konkret ödəniş əməliyyatına aid risk göstəricilərinin birlikdə qiymətləndirilməsi tələb olunur. Daha geniş şəkildə desək, Qaydanın 4.4-cü bəndinə uyğun olaraq hesablanmış ödəniş əməliyyatları üzrə fırıldaqçılıq dərəcəsi Qaydaya 1 nömrəli Əlavədə müəyyən edilmiş hədləri aşmamalıdır. Eyni zamanda, həyata keçirilən ödəniş əməliyyatının məbləği də həmin Əlavədə müvafiq fırıldaqçılıq göstəricisi üçün nəzərdə tutulmuş məbləğ limitindən yüksək olmamalıdır. Bu iki meyar risk əsaslı istisnanın tətbiqi üçün ilkin statistik şərtləri təşkil edir.

Bununla yanaşı, Qaydada konkret ödəniş əməliyyatı üzrə qiymətləndirilməli olan risk indikatorları da ayrıca müəyyən edilmişdir. Risk əsaslı istisnanın tətbiqi həmin indikatorların mövcud olmaması ilə şərtləndirilir. Bu məqsədlə aşağıdakı halların mövcud olmaması tələb olunur:

-ödəniş xidməti istifadəçisinin qeyri-adi xərcləmə və ya davranış modelinin müşahidə edilməsi;

-istifadə olunan texniki cihaz və ya proqram təminatı ilə bağlı qeyri-adi göstəricilərin aşkar edilməsi;

[74] Yuxarıda istinad 4, bənd 4.2.

[75] Yenə orada.

-GMA prosesinin hər hansı mərhələsində zərərverici proqram təminatının müəyyən edilməsi;

-məlum fırıldaqçılıq ssenarilərinə uyğun əlamətlərin aşkar edilməsi;

-ödəniş xidməti istifadəçisinin yerləşdiyi ölkə ilə bağlı risk indikatorlarının mövcudluğu;

-vəsaiti alanın yüksək riskli ölkədə yerləşməsi.

Göründüyü kimi, Qayda aşağı riskli ödəniş əməliyyatının müəyyən edilməsini yalnız kəmiyyət meyarlarına deyil, həm də istifadəçinin davranışı, texniki təhlükəsizlik göstəriciləri və coğrafi risk faktorlarının birlikdə qiymətləndirilməsinə əsaslandırır.[76] Bu isə monitorinq mexanizminin sadəcə fırıldaqçılıq statistikasına əsaslanan sistem deyil, real vaxt rejimində müxtəlif risk indikatorlarını təhlil edən kompleks risk idarəetmə mexanizmi olduğunu göstərir.

Monitorinq mexanizmi vasitəsilə risk əsaslı istisnanın tətbiqi ödəniş xidməti təchizatçılarının mülahizəsinə tam şəkildə buraxılmamışdır. Əksinə, Qayda bu istisnanın tətbiqinin davamlı olaraq monitorinq edilməsini təmin edən nəzarət mexanizmi müəyyən etmişdir. Bu məqsədlə ödəniş xidməti təchizatçıları rüblük əsasda fırıldaqçılıq göstəricilərini hesablamalı və bu göstəriciləri illik hesabatın tərkib hissəsi kimi nəzarət orqanına təqdim etməlidirlər.[77] Həmin göstəricilər Qaydaya 1 nömrəli Əlavədə müəyyən edilmiş hədləri aşdığı halda, müvafiq əməliyyat kateqoriyası üzrə GMA istisnasının tətbiqi dərhal dayandırılır. Diqqətəlayiq hal ondan ibarətdir ki, fırıldaqçılıq göstəricisi hesablanarkən ödəniş xidməti istifadəçisinin vəsaitinin sonradan geri qaytarılması və ya dəymiş zərərin kompensasiya edilməsi nəzərə alınmır.

Azərbaycan Respublikasında müəyyən edilmiş risk əsaslı istisna mexanizmi RTS-də nəzərdə tutulan əməliyyat riskinin təhlili (Transaction Risk Analysis – TRA) yanaşması ilə əhəmiyyətli oxşarlıq təşkil edir. Belə ki, hər iki tənzimləmədə risk əsaslı istisnanın tətbiqi əməliyyatın məbləği, müəyyən edilmiş fırıldaqçılıq göstəriciləri və konkret əməliyyat üzrə aparılan risk təhlilinin nəticələri ilə əlaqələndirilir. Bununla belə, fırıldaqçılıq göstəricisinin müəyyən edilmiş həddi aşmasının hüquqi nəticələri baxımından iki tənzimləmə arasında fərq mövcuddur.

RTS-nin 20-ci maddəsinə əsasən, monitorinq edilən fırıldaqçılıq göstəricisi müəyyən edilmiş istinad həddini aşdıqda ödəniş xidməti təchizatçısı ilkin olaraq bu barədə səlahiyyətli orqana dərhal məlumat verməli və göstəricinin müəyyən edilmiş həddə qaytarılması üçün nəzərdə tutulan tədbirləri təqdim etməlidir. İstisnanın tətbiqinin dayandırılması isə fırıldaqçılıq göstəricisinin müvafiq həddi ardıcıl iki rüb ərzində aşması halında tələb olunur. Azərbaycan GMA Qaydasında isə müvafiq fırıldaqçılıq göstəricisinin

[76] Yenə orada, yarımbənd 4.2.3.

[77] Yenə orada, bənd 4.4.

müəyyən edilmiş həddi aşması risk əsaslı istisnanın tətbiqinin dərhal dayandırılmasına səbəb olur.[78] Bu baxımdan Azərbaycan tənzimləməsi istisnanın dayandırılması üçün RTS ilə müqayisədə daha sərt yanaşma müəyyən edir.

Bu yanaşma ödəniş təhlükəsizliyinin təmin edilməsi baxımından üstünlük təşkil etsə də, fırıldaqçılıq göstəricisinin yalnız bir rüb ərzində normativ həddi cüzi və ya müvəqqəti şəkildə aşması nəticəsində risk əsaslı istisnanın dərhal dayandırılmasına səbəb ola bilər. Bu baxımdan RTS-də olduğu kimi, həddin ilk dəfə aşılması zamanı ödəniş xidməti təchizatçısının nəzarət orqanını məlumatlandırması və göstəricinin normativ həddə qaytarılması üçün tədbirlər planı təqdim etməsi, istisnanın məcburi dayandırılmasının isə göstəricinin müəyyən müddət ərzində normativ həddən yüksək qalması ilə əlaqələndirilməsi imkanının nəzərdən keçirilməsi məqsədəuyğun ola bilər. Belə yanaşma təhlükəsizlik tələbləri ilə risk əsaslı istisnanın səmərəli tətbiqi arasında daha çevik balansın təmin edilməsinə xidmət edə bilər.

Monitorinq mexanizminin effektiv tətbiqini təmin etmək məqsədilə Qayda onun təşkilinə dair əlavə tələblər də müəyyən etmişdir. Belə ki, Qayda emitentlərə monitorinq funksiyasının müqavilə əsasında ödəniş sistemi operatoruna həvalə edilməsinə imkan versə də, bu, onların qanunvericilikdən, o cümlədən cinayət yolu ilə əldə edilmiş əmlakın leqallaşdırılması və terrorçuluğun maliyyələşdirilməsinə qarşı mübarizə sahəsində irəli gələn öhdəliklərini aradan qaldırmır. Həmçinin Qaydanın keçid müddəalarına əsasən, ödəniş xidməti təchizatçıları mövcud monitorinq sistemlərini 1 yanvar 2025-ci il tarixinədək Qaydanın 4.1-ci bəndinin tələblərinə uyğunlaşdırmalı idilər. Bu tələbin müəyyən edilməsi monitorinq mexanizminin GMA sisteminin ayrılmaz hissəsi kimi qəbul edildiyini və onun effektiv tətbiqinin qanunverici tərəfindən xüsusi əhəmiyyət kəsb etdiyini göstərir.

Beləliklə, monitorinq funksiyasının icrası üçün texniki fəaliyyət üçüncü şəxsə həvalə oluna bilsə də, həmin funksiyanın qanunvericiliyə uyğun həyata keçirilməsinə görə hüquqi məsuliyyət emitentin üzərində qalır.

IV. GMA institutunun təkmilləşdirilməsinə dair təkliflər

Məqalədə aparılan təhlil göstərir ki, Azərbaycan qanunvericiliyində GMA ilə bağlı əsas qaydalar müəyyən edilsə də, bəzi məsələlərin daha aydın tənzimlənməsinə ehtiyac var. Xüsusilə autentifikasiya elementlərinin müəyyən edilməsi, onların müstəqilliyi və risk əsaslı yanaşmanın tətbiqi baxımından bir sıra suallar yaranır. Bu baxımdan aşağıdakı təkliflər nəzərdən keçirilə bilər:

[78] Yenə orada, bənd 4.5.

A. GMA elementlərinin müəyyən edilməsi

Məqalədə aparılan təhlildən göründüyü kimi, müəyyən məlumat və vasitənin "bildiyi", "sahib olduğu" və ya "məxsus olduğu" elementlərindən birinə aid edilməsi yalnız həmin məlumat və ya vasitənin formal xüsusiyyətinə əsaslanmamalıdır. Belə ki, autentifikasiya elementinin düzgün müəyyən edilməsi həmin məlumat və ya vasitənin faktiki tətbiq mexanizminin, məxfiliyinin təmin olunması imkanlarının və müştərinin şəxsiyyətinin etibarlı şəkildə təsdiqlənməsində oynadığı rolun qiymətləndirilməsini tələb edir. Məqalədə birdəfəlik şifrələrin, mobil cihazların və biometrik məlumatların təhlili də göstərir ki, autentifikasiya vasitəsinin hüquqi qiymətləndirilməsi onun konkret tətbiq xüsusiyyətlərindən asılıdır.

Xüsusilə, üçüncü şəxslər tərəfindən əldə edilə bilən məlumatların "bildiyi", kart nömrəsi, son istifadə tarixi və statik CVV kimi məlumatların isə avtomatik olaraq "sahib olduğu" elementi hesab edilməsi GMA-nın təhlükəsizlik məqsədi ilə uyğun gəlmir.

Bu cür qeyri-müəyyənliklər ödəniş xidməti təchizatçıları tərəfindən eyni autentifikasiya mexanizminin fərqli qiymətləndirilməsinə və nəticədə GMA tələblərinin qeyri-bərabər tətbiqinə səbəb olur. Bundan əlavə, autentifikasiya elementlərinin yanlış təsnif edilməsi nəticəsində iki elementdən istifadə olunsa belə, onların tələb olunan təhlükəsizlik səviyyəsini faktiki olaraq təmin etməməsi riski yaranır.

Bu səbəbdən, GMA Qaydasında və ya onun tətbiqinə dair izahlarda hər bir autentifikasiya elementinin müəyyən edilməsi üçün daha konkret meyarların və praktiki nümunələrin təqdim edilməsi məqsədəuyğun olar. Belə meyarlar hazırlanarkən məlumatın və ya vasitənin müştəri ilə əlaqəsi, üçüncü şəxslərin ona çıxış imkanları, autentifikasiya prosesində yerinə yetirdiyi funksiya və digər elementlərdən müstəqilliyi nəzərə alınmalıdır. Bu yanaşma autentifikasiya elementlərinin yalnız formal deyil, funksional xüsusiyyətləri əsasında qiymətləndirilməsinə və GMA-nın təhlükəsizlik məqsədinin daha effektiv təmin edilməsinə xidmət edə bilər.

B. GMA-nın tətbiqinə dair vahid izah və praktiki rəhbərliyin hazırlanması

GMA-nın tətbiqi yalnız normativ müddəaların məzmununun müəyyən edilməsini deyil, həmin müddəaların konkret ödəniş modellərinə və texnoloji həllərə necə tətbiq olunacağının müəyyən edilməsini də tələb edir. Məqalədə nəzərdən keçirilən kart məlumatları, elektron cüzdanlar, tokenləşmə, MIT, dövri ödənişlər və digər məsələlər göstərir ki, normativ müddəaların praktiki tətbiqi zamanı müxtəlif interpretasiyaların yaranması mümkündür.

Xüsusilə ödəniş əməliyyatının hansı mərhələsində GMA-nın tələb olunması, müəyyən əməliyyatın GMA-nın tətbiq dairəsinə daxil olub-olmaması və istisnaların hansı şərtlərlə tətbiq edilə bilməsi kimi məsələlər hər

zaman normativ müddəaların mətnindən birbaşa müəyyən edilmir. Bu isə oxşar əməliyyatlara münasibətdə fərqli yanaşmaların formalaşmasına və ödəniş xidməti təchizatçıları üçün hüquqi qeyri-müəyyənliyin yaranmasına səbəb ola bilər.

Avropa İttifaqının təcrübəsində EBA tərəfindən ayrı-ayrı autentifikasiya mexanizmləri və ödəniş modelləri ilə bağlı təqdim edilən izahlar normativ müddəaların praktiki tətbiqinin aydınlaşdırılmasında mühüm rol oynayır. Məqalədə həmin izahlara müraciət edilməsi də göstərir ki, texnoloji inkişafın sürəti nəzərə alındıqda, ümumi normativ tələblərin konkret hallara tətbiqi əlavə şərh mexanizmlərinə ehtiyac yaradır.

Bu baxımdan səlahiyyətli orqan tərəfindən müstəqil şəkildə və ya bazar iştirakçıları ilə əməkdaşlıq çərçivəsində "Ödəniş xidmətləri və ödəniş sistemləri haqqında" Qanunun və GMA Qaydasının tətbiqinə dair vahid izah və praktiki rəhbərliyin hazırlanması məqsədəuyğundur. Belə sənəddə ayrı-ayrı GMA elementləri, onların müstəqilliyi, ödəniş əməliyyatlarının növləri, istisnaların tətbiq şərtləri və müxtəlif praktiki nümunələr üzrə izahlar verilə bilər. Bu cür rəhbərlik ödəniş xidməti təchizatçıları üçün qeyri-müəyyən halların aradan qaldırılmasına, ödəniş xidməti istifadəçilərinin tətbiq olunan autentifikasiya tələblərini daha yaxşı anlamasına, habelə mübahisələr zamanı müvafiq normaların daha şəffaf şərh edilməsinə töhfə verəcəkdir.

C. Risk əsaslı monitorinqin və nəzarət mexanizmlərinin təkmilləşdirilməsi

Məqalədə GMA-nın tətbiqindən risk əsaslı istisnaların təhlili göstərir ki, həmin istisnaların təhlükəsiz tətbiqi yalnız fırıldaqçılıq göstəricilərinin müəyyən edilmiş hədlər daxilində saxlanılmasından deyil, həm də ödəniş əməliyyatları üzrə risklərin vaxtında aşkar edilməsindən və onlara qarşı müvafiq tədbirlərin görülməsindən asılıdır. Bu baxımdan risk əsaslı istisnaların effektiv tətbiqi həm risklərin müəyyən edilməsi və monitorinqi, həm də aşkar edilmiş risklərə münasibətdə mütənasib nəzarət tədbirlərinin həyata keçirilməsini tələb edir.

Mövcud tənzimləmədə ödəniş xidməti təchizatçıları əməliyyatların risk səviyyəsinin müəyyən edilməsini və fırıldaqçılıq göstəricilərinin monitorinqini öz fəaliyyətləri çərçivəsində həyata keçirirlər. Bununla belə, ödəniş fırıldaqçılığı üsullarının müxtəlif ödəniş xidməti təchizatçılarına münasibətdə eyni və ya oxşar formada tətbiq edilə bilməsi ayrı-ayrı təchizatçılar tərəfindən aşkar edilmiş risklərin digər bazar iştirakçıları üçün də əhəmiyyət daşımasına səbəb olur.

Bu səbəbdən, səlahiyyətli dövlət orqanı ilə ödəniş xidməti təchizatçıları arasında fırıldaqçılıq halları və risk indikatorları barədə məlumat mübadiləsini təmin edən mərkəzləşdirilmiş mexanizmin yaradılması nəzərdən keçirilə bilər. Belə mexanizm ayrı-ayrı ödəniş xidməti təchizatçılarında aşkar edilmiş yeni fırıldaqçılıq üsulları və risk indikatorları

barədə digər iştirakçıların daha operativ məlumatlandırılmasına və müvafiq qabaqlayıcı tədbirlərin vaxtında görülməsinə imkan verər. Bu zaman məlumat mübadiləsinin fərdi məlumatların qorunması, bank sirri və digər qanunla qorunan məlumatların məxfiliyinə dair tələblərə uyğun həyata keçirilməsi təmin edilməlidir.

Risk əsaslı monitorinqin təkmilləşdirilməsi ilə yanaşı, monitorinq nəticəsində müəyyən edilmiş fırıldaqçılıq göstəricilərinin normativ hədləri aşması hallarına münasibətdə tətbiq olunan nəzarət mexanizmlərinin də qiymətləndirilməsi məqsədəuyğundur. Belə ki, məqalədə aparılan müqayisəli təhlilə əsasən Azərbaycan Respublikasında GMA-nın tətbiqindən risk əsaslı istisnaların dayandırılması mexanizmi ilə Avropa İttifaqının müvafiq tənzimləməsi arasında müəyyən fərqlər mövcuddur.

Avropa İttifaqının müvafiq tənzimləməsində fırıldaqçılıq göstəricilərinin müəyyən edilmiş hədləri aşması hallarında mərhələli yanaşma nəzərdə tutulur. Belə ki, göstəricinin həddi aşdığı ilk hesabat dövründə nəzarət orqanının məlumatlandırılması, həddin ardıcıl olaraq iki rüb ərzində aşılması halında isə düzəldici tədbirlər planının təqdim edilməsi tələb olunur. Göstəricinin ardıcıl üç rüb ərzində həddi aşması istisnanın tətbiqinin dayandırılmasına səbəb olur. Bu yanaşma ödəniş xidməti təchizatçılarına aşkar edilmiş çatışmazlıqları aradan qaldırmaq imkanı verməklə yanaşı, risklərin davamlı xarakter aldığı hallarda daha sərt nəzarət tədbirlərinin tətbiqini təmin edir.

Bu baxımdan Azərbaycan Respublikasında da fırıldaqçılıq göstəricilərinin müəyyən edilmiş hədləri aşması hallarında risk əsaslı istisnaların tətbiqinin dərhal dayandırılması əvəzinə, Avropa təcrübəsi nəzərə alınmaqla mərhələli nəzarət mexanizminin tətbiqi imkanları qiymətləndirilə bilər. Xüsusilə göstəricinin müəyyən edilmiş həddi ilk dəfə aşması ilə həmin halın ardıcıl hesabat dövrlərində təkrarlanmasının hüquqi nəticələrinin fərqləndirilməsi məqsədəuyğundur. Bu yanaşma ödəniş xidməti təchizatçılarını aşkar edilmiş risklərin aradan qaldırılması üçün vaxtında tədbirlər görməyə təşviq etməklə yanaşı, istisnaların tətbiqinin dayandırılmasını fırıldaqçılıq risklərinin davamlılığı və görülmüş tədbirlərin nəticələri ilə əlaqələndirməyə imkan verər.

D. GMA və onun istisnalarının tətbiqində ödəniş xidməti təchizatçılarının funksiyalarının fərqləndirilməsi

Məqalədə GMA-nın tətbiqindən istisnaların təhlili göstərir ki, müvafiq tələblərin düzgün tətbiqi yalnız ödəniş əməliyyatının növündən deyil, həm də həmin əməliyyatda iştirak edən ödəniş xidməti təchizatçılarının funksiyalarından asılıdır. Müxtəlif ödəniş modellərində bir neçə ödəniş xidməti təchizatçısının iştirak etməsi GMA-nın tətbiqi ilə bağlı vəzifələrin və qərarvermə səlahiyyətlərinin düzgün müəyyən edilməsini zəruri edir.

Avropa İttifaqında GMA ilə bağlı tələblərin praktiki tətbiqinə dair formalaşmış izahlarda ödəniş əməliyyatında iştirak edən ödəniş xidməti təchizatçısının növü və funksiyası nəzərə alınmaqla fərqli yanaşmalar müəyyən edilir. Bu, xüsusilə AISP və PISP-lərin, ödəyicinin və ya vəsait alanın ödəniş xidməti təchizatçısının, habelə ayrı-ayrı hallarda emitent və ekvayerlərin GMA tələblərinin tətbiqində rolunun müəyyənləşdirilməsinə imkan verir.

Azərbaycan qanunvericiliyində isə GMA-nın tətbiqini tənzimləyən Qaydada əsasən ümumi "ödəniş xidməti təchizatçısı" anlayışından istifadə edilir və ayrı-ayrı ödəniş xidməti təchizatçılarının GMA tələblərinin tətbiqində funksiyalarını konkretləşdirən ayrıca tətbiq izahları mövcud deyildir. Bu baxımdan GMA qaydasında və ya tətbiqinə dair izahlarda müvafiq tələblərin ödəniş xidməti təchizatçılarının növü və konkret ödəniş əməliyyatındakı funksiyası nəzərə alınmaqla açıqlanması məqsədəuyğundur. Belə izahlar GMA-nın və onun tətbiqindən istisnaların konkret hallarda hansı ödəniş xidməti təchizatçısı tərəfindən və hansı şərtlərlə tətbiq edilməli olduğunun daha aydın müəyyənləşdirilməsinə kömək edə bilər.

Nəticə

Tədqiqat göstərir ki, Azərbaycan Respublikasında GMA-nın tətbiqi üçün əsas hüquqi çərçivə mövcuddur. Lakin onun effektivliyi autentifikasiya elementlərinin müəyyən edilməsi, istisnaların tətbiqi və risklərin idarə olunması məsələlərinin nə dərəcədə aydın tənzimlənməsindən asılıdır.

Autentifikasiya vasitəsinin GMA elementi kimi qiymətləndirilməsi onun adına və ya formasına deyil, konkret tətbiq xüsusiyyətlərinə və təhlükəsizlik meyarlarına uyğunluğuna əsaslanmalıdır. Bu baxımdan "bildiyi" elementin məxfiliyi, elementlərin müstəqilliyi və əməliyyatın məbləği ilə vəsait alan arasında dinamik əlaqənin yaradılması xüsusi əhəmiyyət daşıyır. Kart rekvizitlərinin mövcudluğu öz-özlüyündə "sahiblik" elementini təsdiq etmir; dinamik CVV kimi vasitələrin uyğunluğu isə onların texniki xüsusiyyətlərinə və təhlükəsizlik tələblərinə cavab verməsinə görə qiymətləndirilməlidir.

PSD2 və RTS ilə müqayisə göstərir ki, milli tənzimləmə GMA-nın əsas prinsipləri üçün hüquqi əsas yaratsa da, bir sıra məsələlərin praktik tətbiqi əlavə aydınlıq tələb edir. Bunlara çoxfunksiyalı cihazlarda elementlərin müstəqilliyi, təchizatçıların müxtəlif əməliyyatlardakı funksiyaları, elektron poçtla verilən ödəniş tapşırıqlarına və vəsait alan tərəfindən başladılan əməliyyatlara (MIT) GMA-nın tətbiqi daxildir. Risk əsaslı istisnalar sahəsində də fərq var: milli Qaydada fırıldaqçılıq göstəricisi həddi aşdıqda istisna dayandırılır, RTS isə mərhələli yanaşma müəyyən edir. Bu fərq istisnalara nəzarət mexanizminin təkmilləşdirilməsi imkanlarının qiymətləndirilməsini zəruri edir. Aşkar edilmiş məsələlərin həlli üçün üç istiqamət təklif olunur. Birincisi, GMA elementlərinin müəyyən edilməsi üzrə konkret meyarlar və praktiki izahlar hazırlanmalıdır. İkincisi, təchizatçıların müxtəlif

əməliyyatlardakı funksiyaları fərqləndirilməli, istisnaların tətbiq şərtləri (o cümlədən MIT və elektron poçtla verilən ödəniş tapşırıqları üzrə) aydınlaşdırılmalıdır. Üçüncüsü, risk əsaslı istisnalara nəzarət mərhələli mexanizm əsasında təkmilləşdirilməli, təchizatçılar arasında risk məlumatlarının mübadiləsi üçün vahid mexanizm qurulmalıdır. Bu tədbirlər vahid izah və praktiki rəhbərlikdə əks olunmalı, hazırlanarkən isə PSD2 və RTS təcrübəsi Azərbaycan ödəniş bazarının xüsusiyyətləri və milli tənzimləmə ilə uzlaşdırılmalıdır.

Beləliklə, GMA-nın effektiv tətbiqi yalnız əsas hüquqi tələblərin müəyyən edilməsi ilə deyil, onların konkret ödəniş əməliyyatlarına və texnoloji vasitələrə tətbiqinin aydınlaşdırılması ilə də bağlıdır. Müəyyən edilmiş hüquqi və praktiki məsələlərin aradan qaldırılması GMA-nın tətbiqində hüquqi müəyyənliyin və risklərin idarə edilməsinin gücləndirilməsinə töhfə verə bilər.