

**Azərbaycan Respublikası Mərkəzi Bankının İdarə Heyətinin
QƏRARI**

№ 12/2

Bakı şəhəri

"13" mart 2024-cü il

"Gücləndirilmiş müştəri autentifikasiyasının tətbiqi Qaydası"nın təsdiq edilməsi barədə

"Ödəniş xidmətləri və ödəniş sistemləri haqqında" Azərbaycan Respublikası Qanununun 35-ci maddəsinə və "Azərbaycan Respublikasının Mərkəzi Bankı haqqında" Azərbaycan Respublikası Qanununun 22.1.17-ci maddəsinə əsasən Azərbaycan Respublikası Mərkəzi Bankının İdarə Heyəti

QƏRARA ALIR:

"Gücləndirilmiş müştəri autentifikasiyasının tətbiqi Qaydası" təsdiq edilsin (əlavə olunur).

Hüquq departamentinə tapşırılsın ki, bu Qərarın 3 gün müddətində Azərbaycan Respublikasının Hüquqi Aktların Dövlət Reyestrinə daxil edilməsi üçün Azərbaycan Respublikasının Ədliyyə Nazirliyinə təqdim edilməsini təmin etsin.

Mərkəzi Bankın sədri

Taleh Kazımov

13 mart 2024-cü il

Gücləndirilmiş müştəri autentifikasiyasının tətbiqi Qaydası

1. Ümumi müddəalar

1.1. Bu Qayda “Ödəniş xidmətləri və ödəniş sistemləri haqqında” Azərbaycan Respublikası Qanununun (bundan sonra – Qanun) 35-ci maddəsinə əsasən hazırlanmışdır və gücləndirilmiş müştəri autentifikasiyasının (bundan sonra - GMA) tətbiqinin tələb edilmədiyi halları və ödəniş xidməti təchizatçılarının xidmətlərindən istifadə olunarkən tətbiq edilən GMA ilə bağlı tələbləri müəyyən edir.

1.2. Ödəniş xidməti təchizatçısının fəaliyyətinin bu Qaydadan irəli gələn tələblərə uyğunluğu daxili audit xidməti tərəfindən ən azı ildə 1 (bir) dəfə yoxlanılmalı və yoxlama üzrə hesabat hər il yanvarın 15-dən gec olmayaraq Mərkəzi Banka təqdim edilməlidir. Daxili auditin yoxlama üzrə hesabatı bu Qaydanın tələbləri üzrə qiymətləndirməni, habelə fırıldaqçılıq dərəcələrinin hesablanması və tələblərə uyğunluğu əks etdirməlidir.

1.3. Bu Qaydada istifadə olunan GMA və digər anlayışlar Qanunda müəyyən edilmiş mənaları ifadə edir.

2. GMA-nın tətbiqi üzrə tələblər

2.1. GMA-nın tətbiqi yalnız ödəniş xidməti istifadəçisinin bildiyi, sahib olduğu və ona məxsus olan elementlərdən iki və ya daha çoxunun istifadəsi nəticəsində həyata keçirilir.

2.2. GMA-nın tətbiqi zamanı ödəniş xidməti təchizatçısı tərəfindən aşağıdakılar təmin edilməlidir:

2.2.1. GMA-nın tətbiqi üçün istifadə edilən bu Qaydanın 2.1-ci bəndində müəyyənləşdirilən elementlərin səlahiyyətli olmayan şəxslər tərəfindən aşkarlanması və istifadəsi mümkün olmamalıdır;

2.2.2. GMA-nın tətbiqi üçün ödəniş xidməti istifadəçisi tərəfindən daxil edilən şifrələrin (birdəfəlik şifrələr istisna olmaqla) gizlədilməsi və ya tam həcmdə oxunmaması təmin edilməlidir;

2.2.3. GMA-nın tətbiqi ilə həyata keçirilən əməliyyatlar üzrə ödəniş alətinin bloklaşdırılması (ödəniş hesabına çıxış imkanının məhdudlaşdırılması) ilə nəticələnən istifadəçiyə icazə verilən ardıcıl uğursuz autentifikasiya cəhdlərinin sayı 3-dən (üç) çox olmamalıdır. Ödəniş xidməti təchizatçısı ödəniş xidməti istifadəçisini bloklaşdırma barədə mümkün olduqda icazə verilən sonuncu autentifikasiya cəhdindən əvvəl və ya ən gec bloklaşdırmadan dərhal sonra məlumatlandırılmalıdır;

2.2.4. GMA-nın tətbiqi zamanı istifadə olunan kommunikasiya sessiyasının səlahiyyətli olmayan şəxslər tərəfindən ələ keçirilməsi və (və ya) dəyişdirilməsi mümkün olmamalıdır;

2.2.5. GMA tətbiq olunaraq ödəniş hesabına daxil olduqdan sonra hər hansı fəaliyyət həyata keçirilmədən aktiv saxlanılan sessiya müddəti mobil tətbiqlər üçün 5 (beş) dəqiqədən, internet bankçılıq üçün isə 30 (otuz) dəqiqədən çox olmamalıdır.

2.3. Ödəniş əməliyyatının elektron formada məsafədən həyata keçirilməsi zamanı ödəniş xidməti təchizatçısı əməliyyatın məbləğinə və vəsait alana dinamik bağlı olan elementlərdən ibarət GMA-nı tətbiq etməlidir.

2.4. Ödəniş terminalları vasitəsilə nağd pul vəsaitinin əldə olunması GMA tətbiq edilməklə həyata keçirilməlidir.

2.5. GMA-nın hər hansı elementi üçün ödəniş xidməti təchizatçısı tərəfindən təqdim edilən proqram təminatı istifadə olunduğu halda, ödəniş xidməti təchizatçısı müvafiq proqram təminatının kənar müdaxilələrdən qorunmasını təmin etməlidir.

3. GMA-nın tətbiqi üzrə istisnalar

3.1. Aşağıdakı əməliyyatlar GMA tətbiq edilmədən həyata keçirilə bilər:

3.1.1. ödəniş hesab(lar)ının balansına dair məlumat əldə edilməsi;

3.1.2. ödəniş hesab(lar)ı üzrə son 180 (bir yüz səksən) gün ərzində aparılan ödəniş əməliyyatlarına dair məlumatın əldə edilməsi.

3.2. Aşağıdakı hallardan azı biri olduqda halda, bu Qaydanın 3.1-ci bəndində müəyyənləşdirilən istisnalar tətbiq edilmir:

3.2.1. ödəniş xidməti istifadəçisi bu Qaydanın 3.1-ci bəndində qeyd edilən məlumatları məsafədən ilk dəfə əldə etdikdə;

3.2.2. ödəniş xidməti istifadəçisinin GMA-nın tətbiqi ilə bu Qaydanın 3.1.2-ci yarımbəndində qeyd edilən əməliyyat üçün ödəniş hesabına daxil olmasından 180 (bir yüz səksən) gündən çox zaman keçdikdə;

3.2.3. müştərinin həssas ödəniş məlumatları açıqlandıqda.

3.3 Ödəniş alətlərinin mobil tətbiqlərə və digər proqram təminatlarına əlavə edilməsi GMA tətbiq edilmədən həyata keçirilə bilər.

3.4. Ödəniş hesabına daxil olmaq üçün GMA tətbiq edildikdə və eyni fasiləsiz sessiya çərçivəsində GMA tələb edən əməliyyat aparıldıqda, həmin əməliyyat GMA tətbiq edilmədən həyata keçirilə bilər.

3.5. Bir təmassız ödənişin məbləği 100 (bir yüz) manat (və ya ekvivalentindən), bu cür əməliyyatların günlük həcmi isə 500 (beş yüz) manat və ya ekvivalentindən çox olmadıqda ödəniş xidməti təchizatçısı GMA tətbiq etməyə bilər.

3.6. Bu Qaydanın 3.7-ci bəndinin tələbləri nəzərə alınmaqla, ödəyici tərəfindən "etibar edilən şəxslər (GMA tətbiq edilmədən xeyrinə ödəniş əməliyyatının həyata keçirildiyi şəxslər) siyahısı"na və dövrü ödənişlər siyahısına daxil edilmiş ödənişlər GMA tətbiq edilmədən həyata keçirilə bilər.

3.7. "Etibar edilən şəxslər siyahısı"nın və dövrü ödənişlər siyahısının tərtib edilməsi və ya mövcud siyahılara dəyişikliklərin edilməsi zamanı GMA tətbiq edilməlidir.

3.8. Ödəniş xidməti istifadəçisinin bir ödəniş xidməti təchizatçısında xidmət olunan ödəniş hesabları arasında aparılan kredit köçürmələri zamanı GMA tətbiq edilməyə bilər.

3.9. Sonuncu GMA tətbiqi ilə həyata keçirilən ödəniş əməliyyatından sonra ardıcıl olaraq məsafədən həyata keçirilən ödəniş əməliyyatlarının sayı beşdən və ya ümumi həcmi 300 (üç yüz) manat və ya ekvivalentindən çox olmadıqda 60 (altmış) manat və ya ekvivalentindən çox olmayan məbləğdə ödəniş əməliyyatı GMA tətbiq edilmədən aparıla bilər.

3.10. Bu Qaydanın 4.5-ci bəndinin tələbi nəzərə alınmaqla, ödəniş xidməti təchizatçısı tərəfindən bu Qaydanın 4.2-ci bəndinə əsasən aşağı riskli hesab olunan ödəniş əməliyyatları GMA tətbiq edilmədən aparıla bilər.

3.11. Ödəniş xidməti təchizatçısı tərəfindən hüquqi şəxslər üçün yaradılan və təhlükəsizlik üzrə zəruri tədbirlərin tətbiq edildiyi xüsusi ödəniş kanalları vasitəsilə aparılan ödənişlər zamanı GMA tətbiq edilməyə bilər.

3.12. Elektron ticarətlə bağlı həyata keçirilən ödəniş əməliyyatları 2026-cı ilin 1 yanvar tarixinədək GMA tətbiq edilmədən həyata keçirilə bilər.

3.13. Bu Qaydanın 3.1-ci, 3.3-cü, 3.4-cü və 3.12-ci bəndlərində nəzərdə tutulan əməliyyatlar həyata keçirilərkən təhlükəsizliyin təmin edilməsi məqsədilə ödəniş xidməti təchizatçıları tərəfindən autentifikasiya həyata keçirilməlidir.

4. Monitoring

4.1. Ödəniş xidməti təchizatçısı avtorizə edilməmiş və ya fırıldaqçılıq əməliyyatlarını aşkar edən əməliyyatların monitoringi mexanizminə sahib olmalıdır. Bu mexanizm hər bir əməliyyat üzrə aşağıdakılar nəzərə alınmaqla monitoring aparılmasını təmin etməlidir:

4.1.1. məxfiliyi pozulmuş və ya oğurlanmış autentifikasiya elementləri;

4.1.2. ödəniş xidmətlərinin göstərilməsi ilə bağlı məlum olan fırıldaqçılıq ssenariləri;

4.1.3. autentifikasiya proseduru zamanı hər hansı zərərverici proqram təminatları;

4.1.4. ödəniş hesabına giriş üçün istifadə olunan texniki cihaz və ya proqram təminatı ödəniş xidməti təchizatçısı tərəfindən təmin edildiyi təqdirdə, texniki cihazın və ya proqram təminatının istifadəsinə dair loqlar.

4.2. Aşağıdakı şərtlərin hamısına cavab verən ödəniş əməliyyatları aşağı riskli hesab edilir:

4.2.1. bu Qaydanın 4.4-cü bəndinə uyğun olaraq hesablanmış ödəniş əməliyyatı üzrə fırıldaqçılıq dərəcəsi bu Qaydaya 1 nömrəli Əlavədə müəyyənləşdirilən fırıldaqçılıq dərəcələrindən yuxarı olmadıqda;

4.2.2. ödəniş əməliyyatının məbləği bu Qaydaya 1 nömrəli Əlavədə müəyyənləşdirilən fırıldaqçılıq dərəcəsi üzrə müəyyən edilmiş məbləğ limitindən yüksək olmadıqda;

4.2.3. ödəniş xidməti təchizatçısı tərəfindən real vaxt rejimində aparılan risk analizi nəticəsində aşağıdakılardan hər hansı biri aşkar edilmədikdə:

4.2.3.1. ödəniş xidməti istifadəçisinin qeyri-adi xərcləmələri və ya davranış tərzini;

4.2.3.2. ödəniş xidməti istifadəçisinin texniki cihaz və ya proqram təminatına çıxışı üzrə qeyri-adi məlumat;

4.2.3.3. GMA-nın tətbiqinin hər hansı mərhələsində zərərverici proqram təminatı;

4.2.3.4. ödəniş xidmətləri üzrə fırıldaqçılıq ssenarilərindən istifadə;

4.2.3.5. ödəniş xidməti istifadəçisinin yerləşdiyi ölkə üzrə şübhəli hal;

4.2.3.6. vəsaiti alanın yüksək risk qrupuna aid edilən ölkədə olması.

4.3. Ödəniş xidməti təchizatçısı rüblük əsasda növbəti ayın ilk 5 (beş) iş günündən gec olmayaraq ödəniş əməliyyatları üzrə fırıldaqçılıq dərəcələrini bu Qaydanın 4.4-cü bəndinə uyğun olaraq hesablamalıdır.

4.4. Pul vəsaitlərinin bərpa edilib-edilməməsindən asılı olmayaraq, fırıldaqçılıq dərəcəsi bu Qaydaya 1 nömrəli Əlavədə müəyyənləşdirilmiş hər bir əməliyyat növü üzrə rüblük əsasda məsafədən səlahiyyətsiz şəkildə və (və ya) fırıldaqçılıqla həyata keçirilən əməliyyatların ümumi həcmninə həmin növ əməliyyatların ümumi həcminə bölünməklə hesablanır. Hesablama zamanı GMA tətbiq edilmədən həyata keçirilən ödəniş əməliyyatları da nəzərə alınır.

4.5. İstənilən növ ödəniş əməliyyatı üzrə fırıldaqçılıq dərəcəsi bu Qaydaya 1 nömrəli Əlavədə müəyyənləşdirilmiş fırıldaqçılıq dərəcəsini keçərsə, ödəniş xidməti təchizatçısı bu Qaydanın 3.10-cu bəndinə əsasən tətbiq edilən istisnadan istifadəni dərhal dayandırmalıdır. Müvafiq istisnadan yenidən istifadəyə yalnız növbəti rüb üzrə hesablanmış ödəniş əməliyyatı üzrə fırıldaqçılıq dərəcəsi bu Qaydaya 1 nömrəli Əlavədə müəyyənləşdirilən fırıldaqçılıq dərəcəsinə uyğun olduqda yol verilə bilər.

4.6. Emitent ödəniş alətləri ilə aparılmış şübhəli əməliyyatlar üzrə monitorinqin keçirilməsini müqavilə əsasında ödəniş sistemi operatoruna həvalə edə bilər. Bu zaman emitent qanunvericilikdə, o cümlədən cinayət yolu ilə əldə edilmiş əmlakın leqallaşdırılmasına və terrorçuluğun maliyyələşdirilməsinə qarşı mübarizə və hədəfli maliyyə sanksiyaları sahəsində qanunvericilikdə, eləcə də ödəniş xidməti istifadəçisi ilə bağlanmış müqavilədə nəzərdə tutulmuş vəzifədən azad edilmir.

5. Yekun müddəalar

Ödəniş xidməti təchizatçıları avtorizə edilməmiş və ya fırıldaqçılıq əməliyyatlarını aşkar edən mövcud monitorinq mexanizmlərinin bu Qaydanın 4.1-ci bəndinin tələbinə uyğunlaşdırılmasını 2025-ci ilin 1 yanvar tarixinədək təmin etməlidirlər.

“Gücləndirilmiş müştəri autentifikasiyasının
tətbiqi Qaydası”na
Əlavə 1

İstisnadan istifadə üçün müəyyən edilmiş məbləğ limiti	İstinad edilən fırıldaqçılıq dərəcəsi (%)	
	Məsafədən həyata keçirilən kart əsaslı ödənişlər üzrə	Məsafədən həyata keçirilən kredit köçürmələri üzrə
500 (beş yüz) manat və ya ekvivalentinə qədər	0.01	0.005
250 (iki yüz əlli) manat və ya ekvivalentinə qədər	0.06	0.01
100 (bir yüz) manat və ya ekvivalentinə qədər	0.13	0.015