

AZƏRBAYCAN RESPUBLİKASININ MƏRKƏZİ BANKI

CbarEdocSigner

Elektron imzanın yaradılması üçün lokal servis

İSTİFADƏÇİ TƏLİMƏTİ

Versiya 2.0

Bakı – 2026

1. Giriş

Bu təlimat CbarEdocSigner lokal servisindən istifadə qaydalarını izah etmək məqsədilə hazırlanmışdır.

CbarEdocSigner proqramı Azərbaycan Respublikasının Mərkəzi Bankının Elektron Sənəd Dövriyyəsi Sistemi (ESDS) ilə inteqrasiya olunaraq elektron imzanın yaradılması prosesini həyata keçirir.

Təlimatda proqramın quraşdırılması, elektron imzanın yaradılması, token PIN kodunun idarə olunması, elektron imzanın yoxlanılması və istifadə zamanı yarana biləcək əsas məsələlər barədə məlumat təqdim olunur.

Sənəd CbarEdocSigner proqramının son istifadəçiləri üçün nəzərdə tutulmuşdur və proqramdan təhlükəsiz və düzgün istifadə qaydalarını əhatə edir.

2. Proqram haqqında

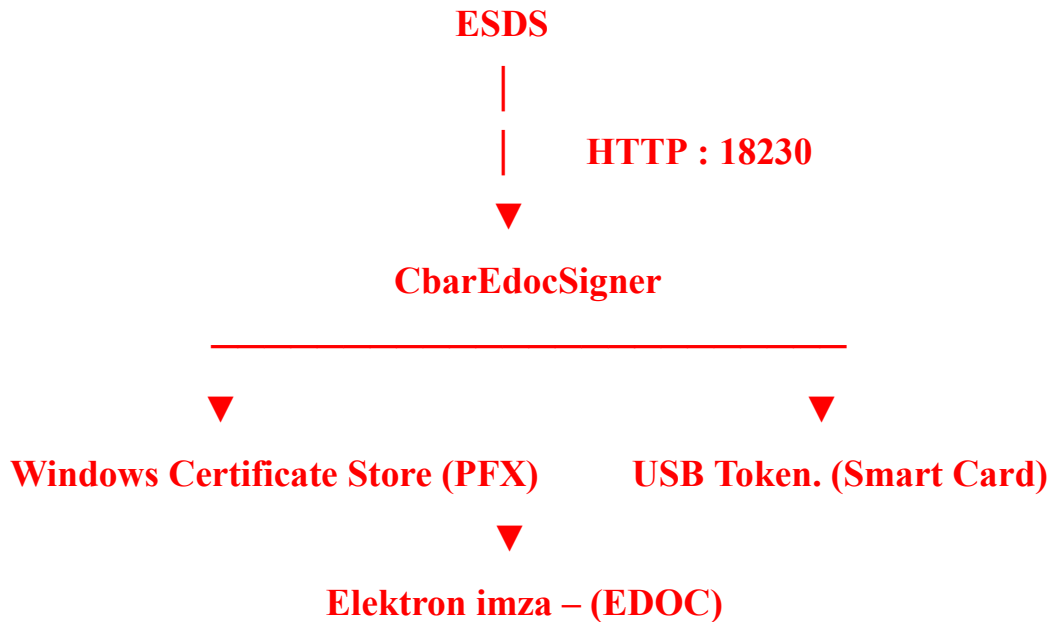
CbarEdocSigner Azərbaycan Respublikasının Mərkəzi Bankının Elektron Sənəd Dövriyyəsi Sistemi (ESDS) ilə işləmək üçün hazırlanmış lokal servis proqramıdır.

Proqram elektron imzanın yaradılması prosesini istifadəçinin kompüterində həyata keçirir və ESDS ilə avtomatik qarşılıqlı əlaqədə işləyir.

CbarEdocSigner proqramının əsas funksiyaları aşağıdakılardır:

- *istifadəçinin elektron sertifikatlarının oxunması;*
- *imzalama üçün uyğun sertifikatın seçilməsi;*
- *elektron imzanın yaradılması;*
- *token PIN kodunun daxil edilməsi və idarə olunması;*

- *təhlükəsizlik tələblərinə cavab verməyən PIN kodunun dəyişdirilməsinin təmin edilməsi;*
- *yaradılmış elektron imzanın yoxlanılması.*



CbarEdocSigner proqramının istifadəçi tərəfindən ayrıca işə salınması tələb olunmur. Quraşdırıldıqdan sonra proqram sistemdə avtomatik olaraq aktiv vəziyyətə gətirilir və elektron imzanın yaradılması tələb olunduqda istifadə edilir.

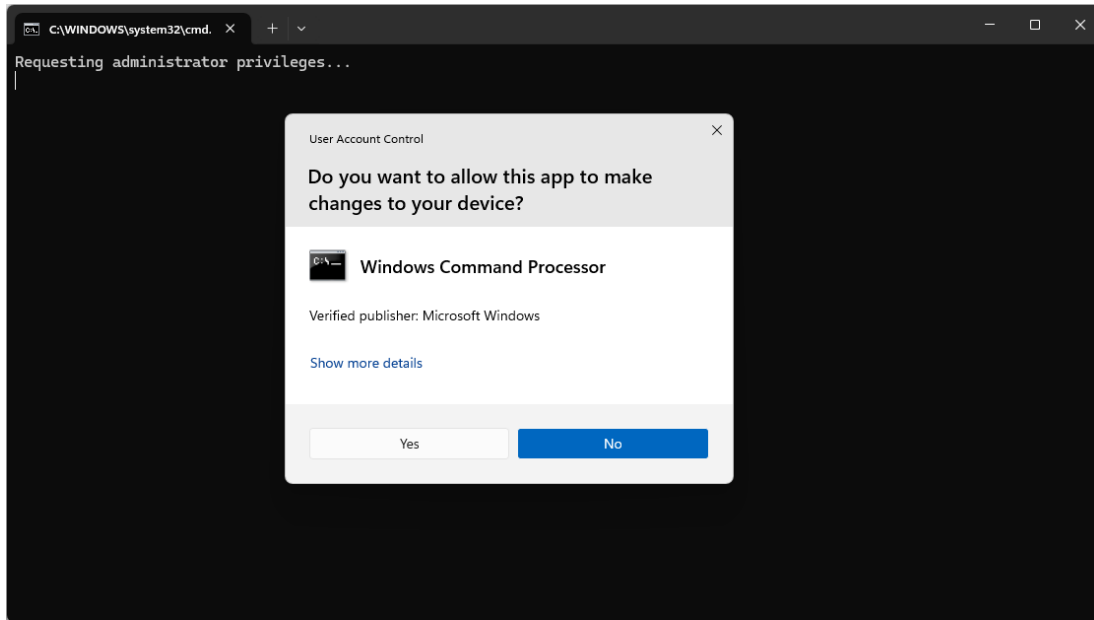
Proqramın quraşdırılması, yenilənməsi və silinməsi avtomatik şəkildə həyata keçirilir. Bu proseslər istifadəçinin əlavə texniki müdaxiləsini və xüsusi texniki biliklərə malik olmasını tələb etmir.

3. Quraşdırma

CbarEdocSigner proqramını quraşdırmaq üçün aşağıdakı quraşdırma faylını işə salın:

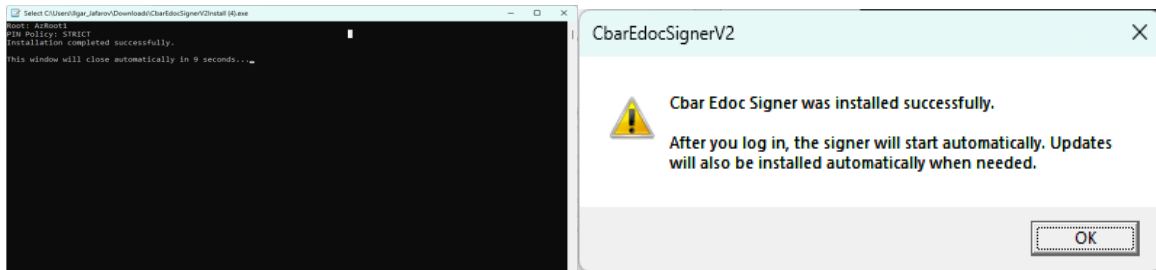
CbarEdocSignerV2Install.exe

Quraşdırma prosesi sistem administratoru tərəfindən həyata keçirilir. Quraşdırma zamanı administrator səlahiyyətləri tələb oluna bilər (Şəkil 1).



Şəkil 1. CbarEdocSigner proqramının quraşdırılması

Quraşdırma prosesi uğurla başa çatdıqdan sonra istifadəçi öz Windows istifadəçi hesabına daxil olmalıdır (Şəkil 2).



Şəkil 2. CbarEdocSigner proqramının quraşdırılmasının tamamlanması

İstifadəçi sistemə daxil olduqdan sonra CbarEdocSigner avtomatik olaraq işə hazır vəziyyətə gətirilir. İstifadəçi tərəfindən əlavə sazlama və ya konfigurasiya tələb olunmur.

3.1. Quraşdırma faylının əldə edilməsi

CbarEdocSigner proqramının quraşdırılması üçün əvvəlcə quraşdırma faylı əldə edilməlidir.

Quraşdırma faylı aşağıdakı ünvanda yerləşir:

<https://csr.cbar.az/download/CbarEdocSignerV2Install.exe>

Quraşdırma faylını kompüterə yüklədikdən sonra faylı işə salın.

3.2. Quraşdırmanın başlatılması

Quraşdırma faylı işə salındıqdan sonra Windows əməliyyat sistemi administrator icazəsi tələb edə bilər.

Administrator icazəsi təsdiqləndikdən sonra quraşdırma prosesi avtomatik olaraq başlayır.

Əgər kompüterdə CbarEdocSigner proqramının əvvəlki versiyası quraşdırılıbsa, yeni versiyanın quraşdırılmasından əvvəl əvvəlki versiya silinməlidir.

Əvvəlki versiya silinmədikdə quraşdırma zamanı 18230 nömrəli portun artıq istifadədə olması ilə bağlı xəbərdarlıq göstərilə bilər.

Bu halda əvvəlki versiyanı silin və quraşdırma prosesini yenidən başlayın.

3.3. Quraşdırmanın tamamlanması

Quraşdırma prosesi başa çatdıqdan sonra əlavə sazlama tələb olunmur.

İstifadəçi Windows sisteminə daxil olduqdan sonra CbarEdocSigner avtomatik olaraq işə hazır vəziyyətə gətirilir.

Proqramın istifadəçi tərəfindən ayrıca işə salınması tələb olunmur.

Elektron imzanın yaradılması tələb olunduqda CbarEdocSigner ESDS ilə avtomatik qarşılıqlı əlaqə yaradaraq imzalama prosesini həyata keçirir.

Qeyd:

CbarEdocSigner proqramının quraşdırılmasından sonra istifadəçi tərəfindən əlavə sazlama, konfigurasiya və ya proqramın əl ilə işə salınması tələb olunmur.

Bütün zəruri proseslər avtomatik şəkildə həyata keçirilir.

3.4. Təhlükəsizlik parametrləri

CbarEdocSigner proqramının quraşdırılması zamanı proqramın təhlükəsizlik siyasətini müəyyən edən policy.json konfigurasiya faylı avtomatik olaraq yaradılır.

Fayl aşağıdakı qovluqda yerləşir:

C:\ProgramData\CbarEdocSignerV2\Admin\policy.json

Konfigurasiya faylında proqramın təhlükəsizlik parametrləri, o cümlədən etibar edilən kök sertifikatların seçimi və token PIN kodunun yoxlanılması siyasəti saxlanılır.

Proqramın ilkin quraşdırılması zamanı "pin_policy" parametrinin dəyəri avtomatik olaraq "FREE" olaraq təyin edilir. FREE rejimində CbarEdocSigner tərəfindən token PIN kodunun mürəkkəbliyi yoxlanılmır.

Təhlükəsizlik baxımından, xüsusi istismar və ya uyğunluq tələbləri olmadığı halda, proqramın quraşdırılmasından sonra "pin_policy" parametrinin "STRICT" olaraq təyin edilməsi tövsiyə olunur.

STRICT rejimində CbarEdocSigner istifadəçinin daxil etdiyi PIN kodunun müəyyən edilmiş təhlükəsizlik tələblərinə uyğunluğunu yoxlayır.

Bu parametrin dəyişdirilməsi Administrator tərəfindən həyata keçirilməlidir. policy.json faylının dəyişdirilməsi yalnız administrator səlahiyyətləri ilə mümkündür.

Qeyd:

Konfigurasiya faylının strukturu dəyişdirilməməli, lazımi parametrlər silinməməli və proqram tərəfindən tanınmayan əlavə parametrlər daxil edilməməlidir. Konfigurasiya parametrlərinin düzgün dəyişdirilməməsi proqramın fəaliyyətinə və təhlükəsizlik siyasətinə təsir göstərə bilər.

3.5. PIN siyasəti parametri

Token PIN kodunun proqram tərəfindən yoxlanılması siyasəti "pin_policy" parametri ilə müəyyən edilir.

Bu parametr aşağıdakı qiymətlərdən birini qəbul edir:

STRICT

PIN kodunun müəyyən edilmiş təhlükəsizlik tələblərinə uyğunluğunun yoxlanıldığı rejimdir.

FREE

PIN kodunun mürəkkəbliyinin CbarEdocSigner tərəfindən yoxlanılmadığı rejimdir.

STRICT rejimi (təvsiyə olunur)

Təhlükəsizlik baxımından, xüsusi istismar və ya uyğunluq tələbləri olmadığı halda STRICT rejimindən istifadə edilməsi təvsiyə olunur.

Nümunə konfigurasiya:

```

{
  "root": "AzRoot1",
  "root_options": {
    "AzRoot1": "SHA1",
    "AzRoot2": "SHA256"
  },
  "pin_policy": "STRICT",
  "pin_policy_options": {
    "STRICT": "strong PIN required",
    "FREE": "no strong PIN required"
  }
}

```

Konfiqurasiya faylında "pin_policy": "STRICT" göstəriləndə, CbarEdocSigner tərəfindən istifadə olunan token PIN kodunun təhlükəsizlik tələblərinə uyğunluğu yoxlanılır.

PIN kodu aşağıdakı tələblərə cavab verməlidir:

- PIN kodunun uzunluğu 8–16 simvol aralığında olmalıdır;
- PIN kodunda ən azı 2 böyük hərflər (A–Z) olmalıdır;
- PIN kodunda ən azı 2 kiçik hərflər (a–z) olmalıdır;
- PIN kodunda ən azı 2 rəqəm (0–9) olmalıdır;
- PIN kodunda ən azı 1 xüsusi simvol olmalıdır.

Xüsusi simvollara nümunələr:

! \$ ^ & * () _ + - = { } [] : ; . , ?

Həmçinin token tərəfindən dəstəklənən digər xüsusi simvollarla istifadə edilə bilər.

PIN kodu:

- istifadəçi adı ilə eyni olmamalıdır;
- ardıcıl və ya təkrarlanan simvollarla ibarət olmamalıdır (məsələn, AAA, 111, 1234);
- əvvəl istifadə edilmiş PIN kodu ilə eyni olmamalıdır.

Qeyd:

Bəzi tokenlər, məsələn ACOS, PIN kodunun uzunluğunu maksimum 8 simvolla məhdudlaşdırır və müəyyən xüsusi simvolları dəstəkləməyə bilər.

Belə hallarda token tərəfindən dəstəklənən PIN formatından istifadə edilməlidir.

FREE rejimi

Proqramın ilkin quraşdırılması zamanı FREE rejimi avtomatik olaraq aktiv edilir.

FREE rejimində CbarEdocSigner tərəfindən token PIN kodunun mürəkkəbliyi yoxlanılır. Bu rejim proqramın ilkin quraşdırılması zamanı tətbiq edilir və PIN kodunun təhlükəsizlik tələblərinə uyğunluğunun proqram tərəfindən məcburi yoxlanılmasını nəzərdə tutmur.

Nümunə konfigurasiya:

```
{  
  "root": "AzRoot1",  
  "root_options": {  
    "AzRoot1": "SHA1",  
    "AzRoot2": "SHA256"
```

```

},
"pin_policy": "FREE",
"pin_policy_options": {
"STRICT": "strong PIN required",
"FREE": "no strong PIN required"
}
}

```

Konfigurasiya faylında "pin_policy": "FREE" göstəriləndə, proqram PIN kodunun mürəkkəbliyini yoxlamır.

Təhlükəsizlik baxımından, xüsusi istismar və ya uyğunluq tələbləri olmadığı halda, Administrator tərəfindən FREE rejiminin STRICT rejiminə dəyişdirilməsi tövsiyə olunur.

3.6. Konfigurasiya faylının yoxlanılması

Proqram hər dəfə işə başladıqda policy.json konfigurasiya faylının düzgünlüyünü yoxlayır.

Aşağıdakı hallarda:

- fayl mövcud olmadıqda;
- fayl zədələndikdə;
- JSON formatı düzgün olmadıqda;
- lazımi parametrlər olmadıqda;
- parametr qiymətləri icazə verilən dəyərlərə uyğun olmadıqda;

proqram avtomatik olaraq ilkin konfigurasiyanı bərpa edir.

İlkin konfigurasiya zamanı "pin_policy" parametrinin dəyəri "FREE" olaraq təyin edilir.

İlkin konfigurasiya:

```
{  
  "root": "AzRoot1",  
  "root_options": {  
    "AzRoot1": "SHA1",  
    "AzRoot2": "SHA256"  
  },  
  "pin_policy": "FREE",  
  "pin_policy_options": {  
    "STRICT": "strong PIN required",  
    "FREE": "no strong PIN required"  
  }  
}
```

Qeyd:

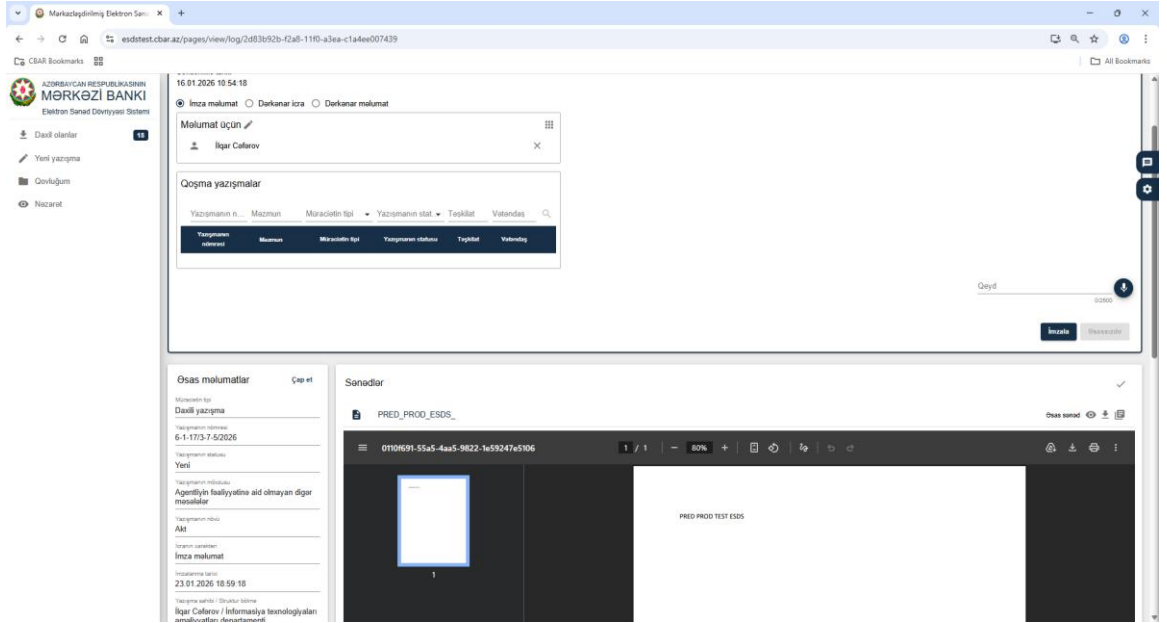
İlkin quraşdırma zamanı FREE rejimi tətbiq olunur və bu rejimdə PIN kodunun mürəkkəbliyi proqram tərəfindən yoxlanılır.

Təhlükəsizlik baxımından, xüsusi istismar və ya uyğunluq tələbləri olmadığı halda STRICT rejimindən istifadə edilməsi tövsiyə olunur.

4. İmzalama prosesi

4.1. Sənədin imzalanmasının başlanılması

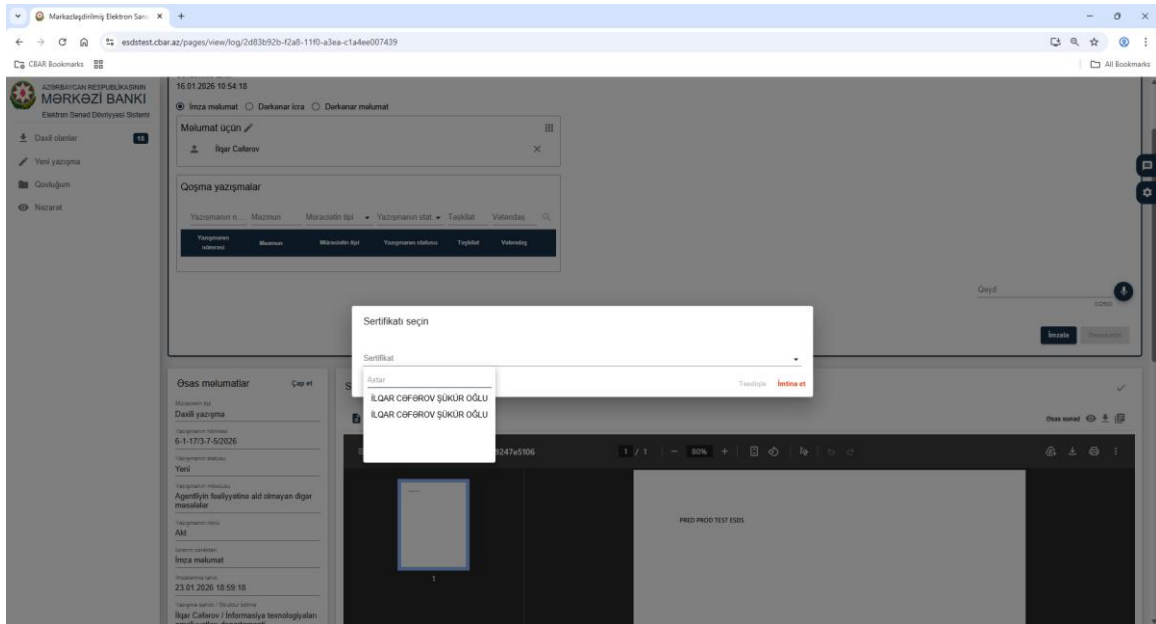
Sənədin elektron imzalanması əməliyyatı ESDS-nin imzalama səhifəsindən başlayır (Şəkil 3).



Şəkil 3. İmzalama sahifəsi

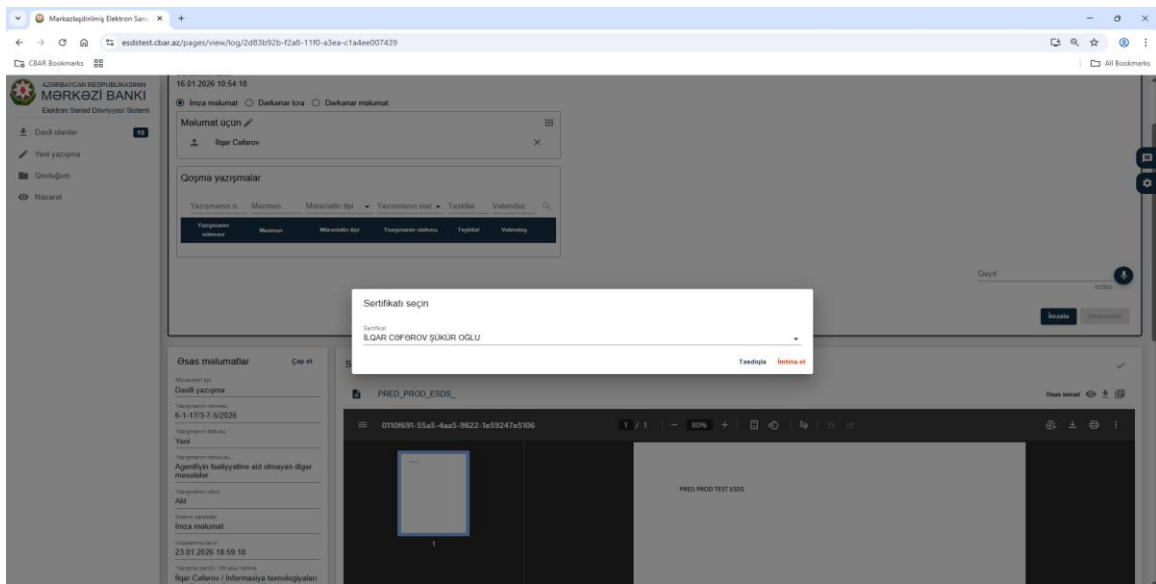
4.2. Sertifikatın seçilməsi

İstifadəçi “İmzala” düyməsini kliklədikdən sonra CbarEdocSigner lokal sertifikat anbarından istifadəçinin mövcud sertifikatlarını oxuyur və imzalama üçün uyğun sertifikatın seçilməsi imkanını təqdim edir (Şəkil 4).



Şəkil 4. Sertifikatın seçilməsi

İstifadəçi sertifikatı seçdikdən və seçimini təsdiqlədikdən sonra ESDS tərəfindən CbarEdocSigner lokal servisində seçilmiş sertifikatın seriya nömrəsi və elektron imzanın yaradılacağı sənədin heş dəyəri JSON formatında POST sorğusu vasitəsilə göndərilir (Şəkil 5).

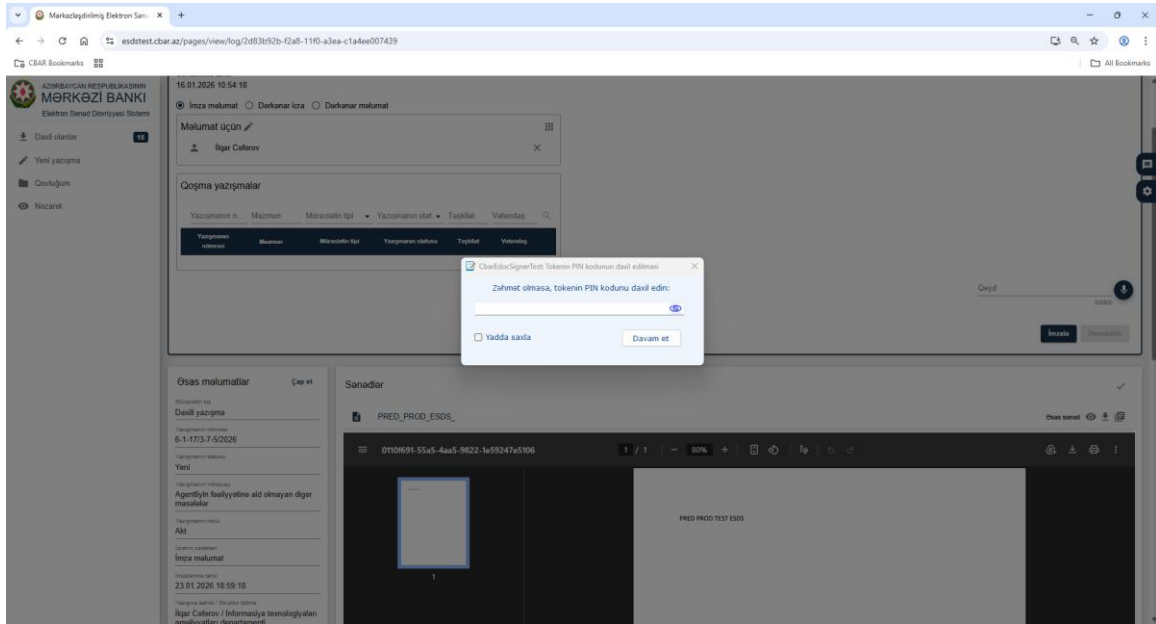


Şəkil 5. Sertifikat seçiminin təsdiqlənməsi

4.3. Token PIN kodunun daxil edilməsi

Əgər PFX formatında sertifikat seçilibsə, CbarEdocSigner sənədin imzalanması prosesinə başlayır.

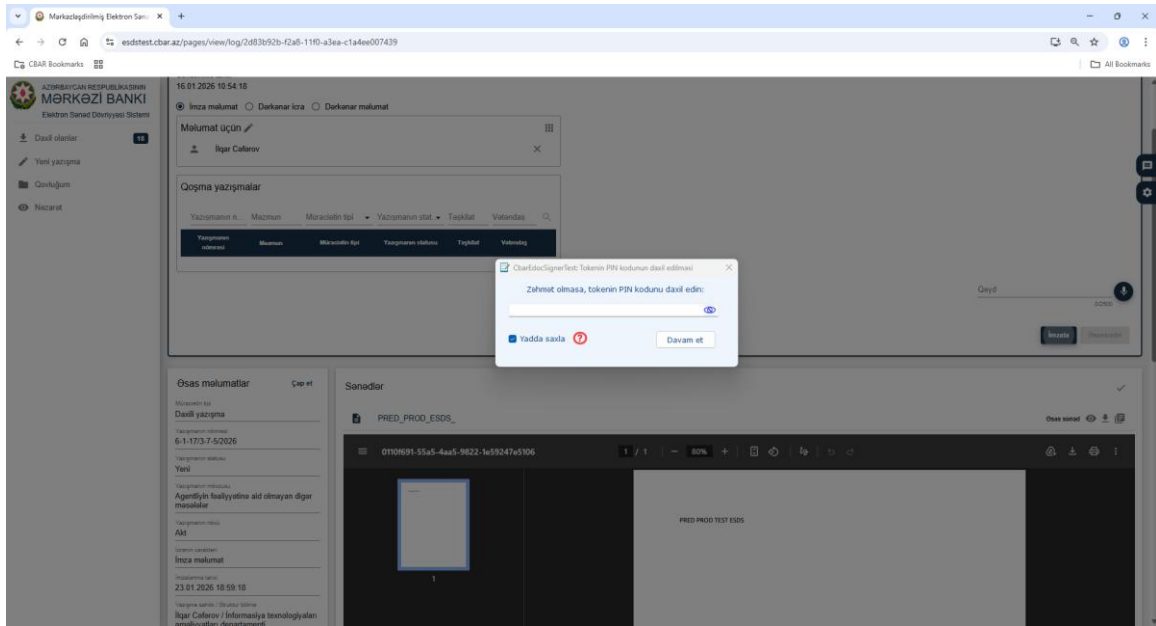
Əgər seçilmiş sertifikat token üzərində yerləşirsə, istifadəçiyə tokenin PIN kodunun daxil edilməsi üçün müvafiq interfeys təqdim olunur (Şəkil 6).



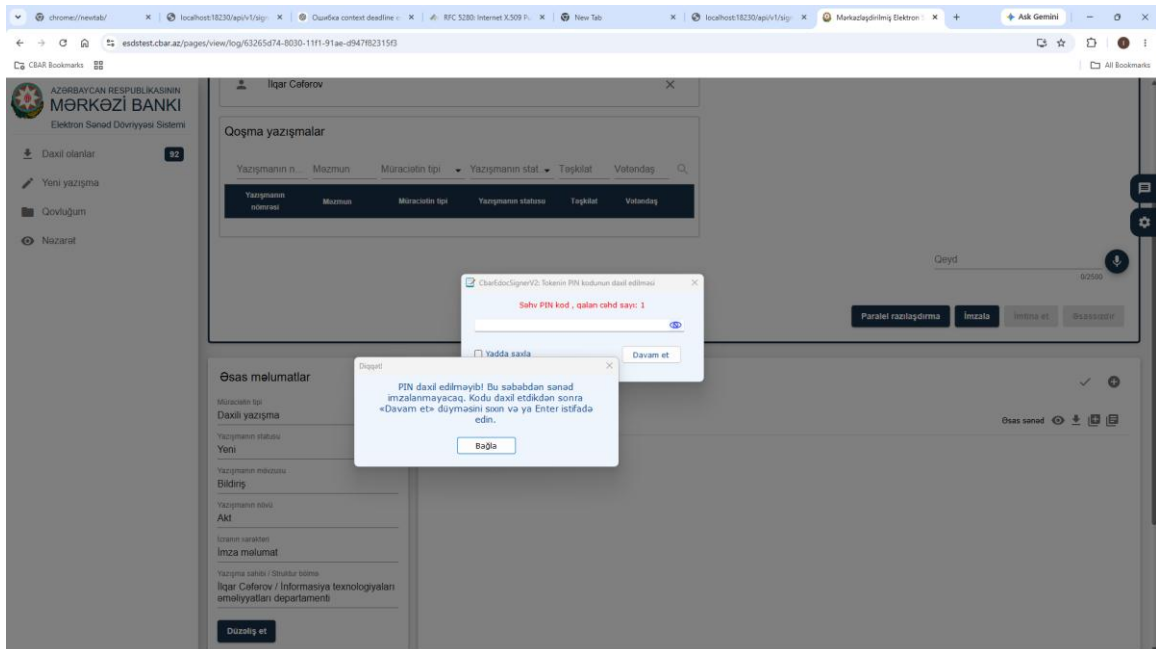
Şəkil 6. PIN kodunun daxil edilməsi

Əgər istifadəçi əvvəlki imzalama əməliyyatı zamanı “PIN kodu yadda saxla” seçimini aktivləşdiribsə və həmin vaxtdan etibarən kompüter yenidən başladılmayıb və istifadəçi sistemdən çıxaraq yenidən daxil olmayıbsa, CbarEdocSigner PIN kodunu yenidən tələb etmədən imzalama əməliyyatını avtomatik həyata keçirə bilər (Şəkil 7).

Bu funksionallıq barədə ətraflı məlumat istifadəçi interfeysində sual işarəsi işarəsinə kliklədikdə göstərilir (Şəkil 8).



Şəkil 7. “PIN kodu yadda saxla” seçimi

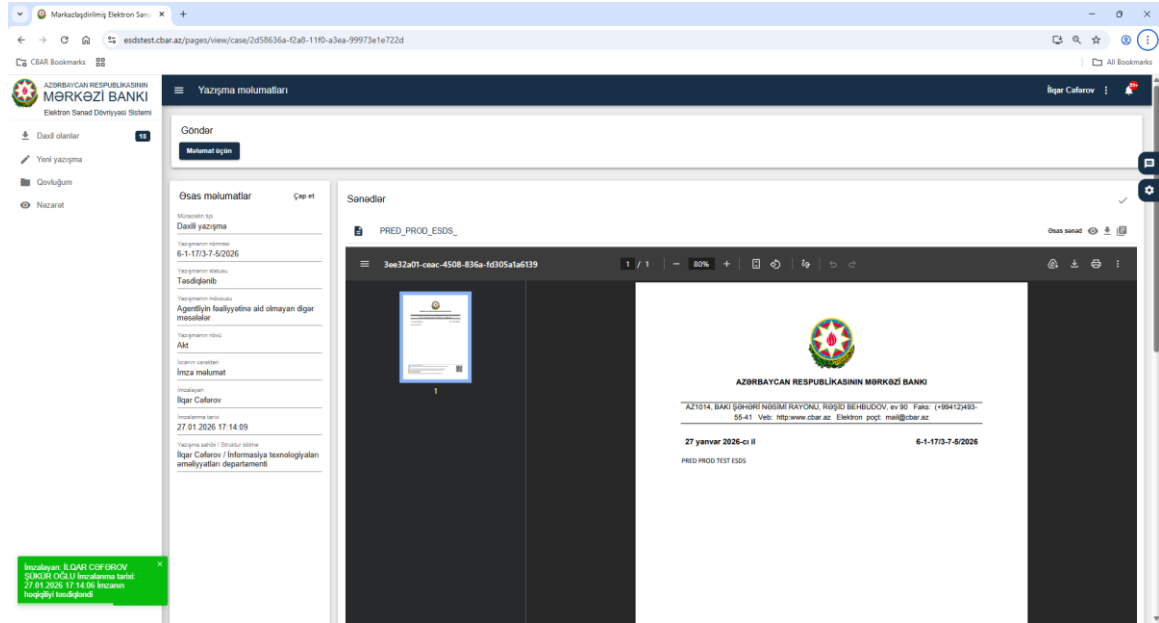


Şəkil 8. “PIN kodu yadda saxla” funksionallığı haqqında məlumat

4.4. Elektron imzanın yoxlanılması

İmzalama prosesi uğurla başa çatdıqdan sonra istifadəçiyə sənədin elektron imzalanmasının uğurla tamamlandığını bildirən məlumat mesajı göstərilir.

“İmzanı yoxla” düyməsinə kliklədikdə elektron sertifikatın sahibi, imzalanma vaxtı və digər müvafiq məlumatlar göstərilir (Şəkil 9).

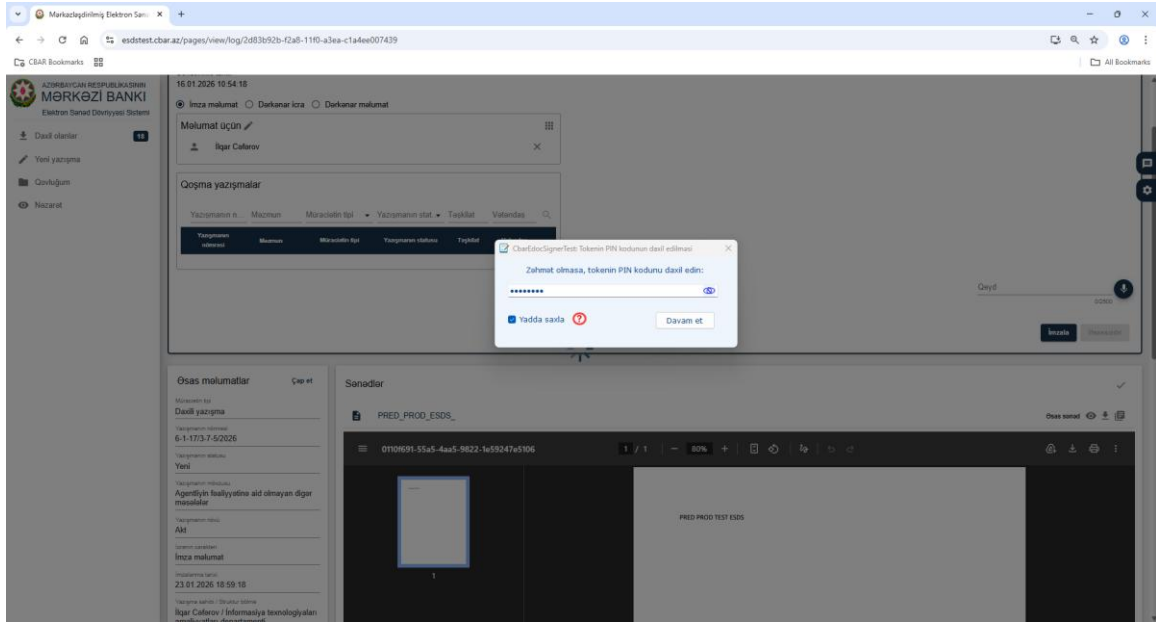


Şəkil 9. Elektron imzanın yoxlanılması

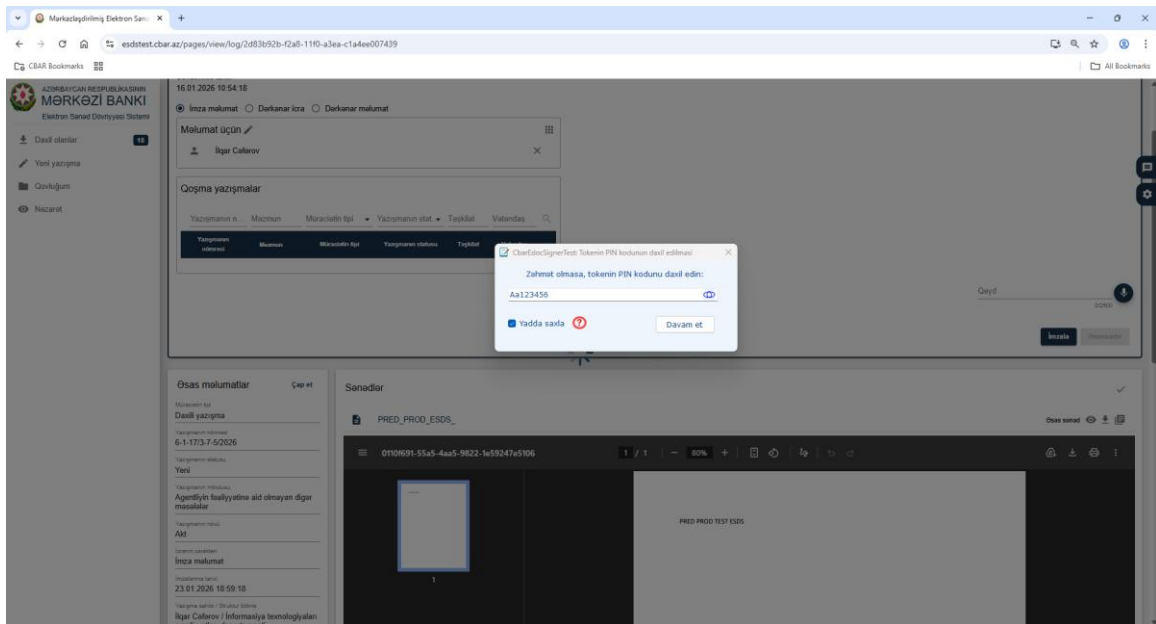
5. Token PIN kodunun dəyişdirilməsi

CbarEdocSigner proqramının əsas təhlükəsizlik funksiyalarından biri token PIN kodunun müəyyən edilmiş təhlükəsizlik tələblərinə uyğunluğunun yoxlanılmasıdır.

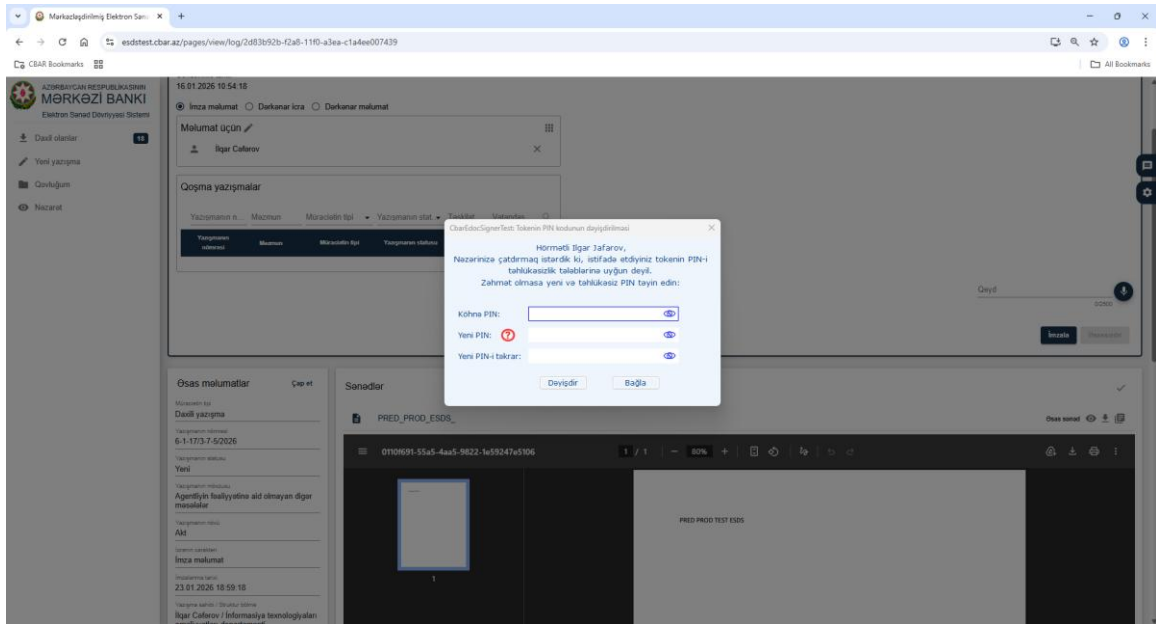
Əgər sənədin imzalanması zamanı istifadə olunan tokenin PIN kodunun təhlükəsizlik tələblərinə uyğun olmadığı müəyyən edilərsə, istifadəçiyə mövcud PIN kodunun daha təhlükəsiz PIN kodu ilə dəyişdirilməsi təklif olunur (Şəkil 10, Şəkil 11, Şəkil 12).



Şəkil 10. “Zəif” PIN kodu ilə imzalama prosesi – Addım 1

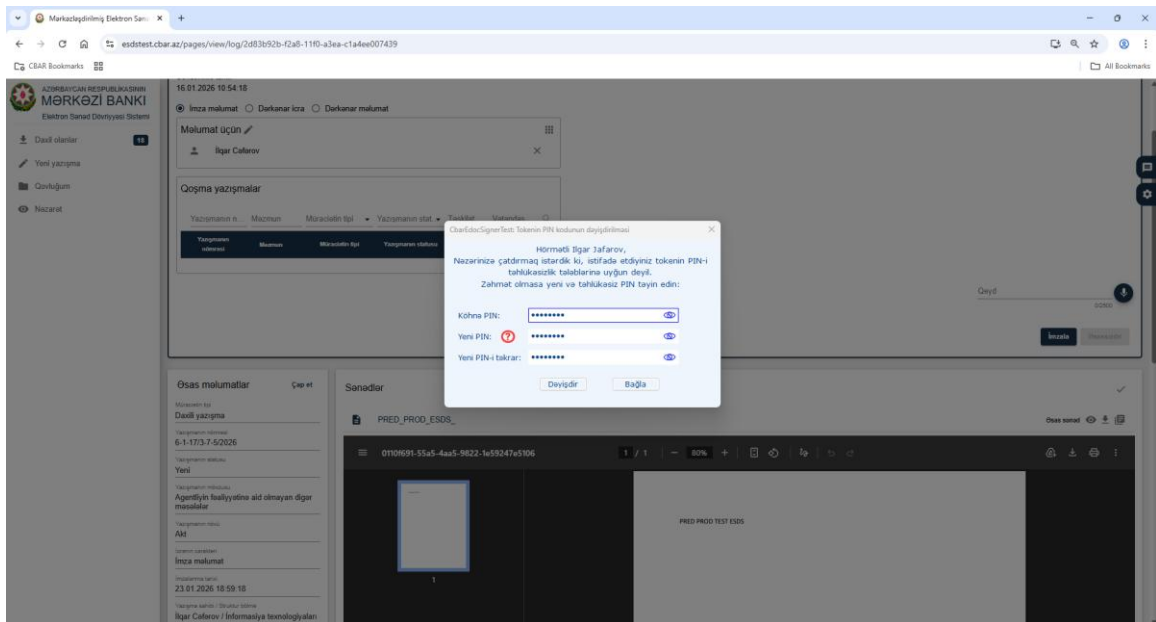


Şəkil 11. “Zəif” PIN kodu ilə imzalama prosesi – Addım 2



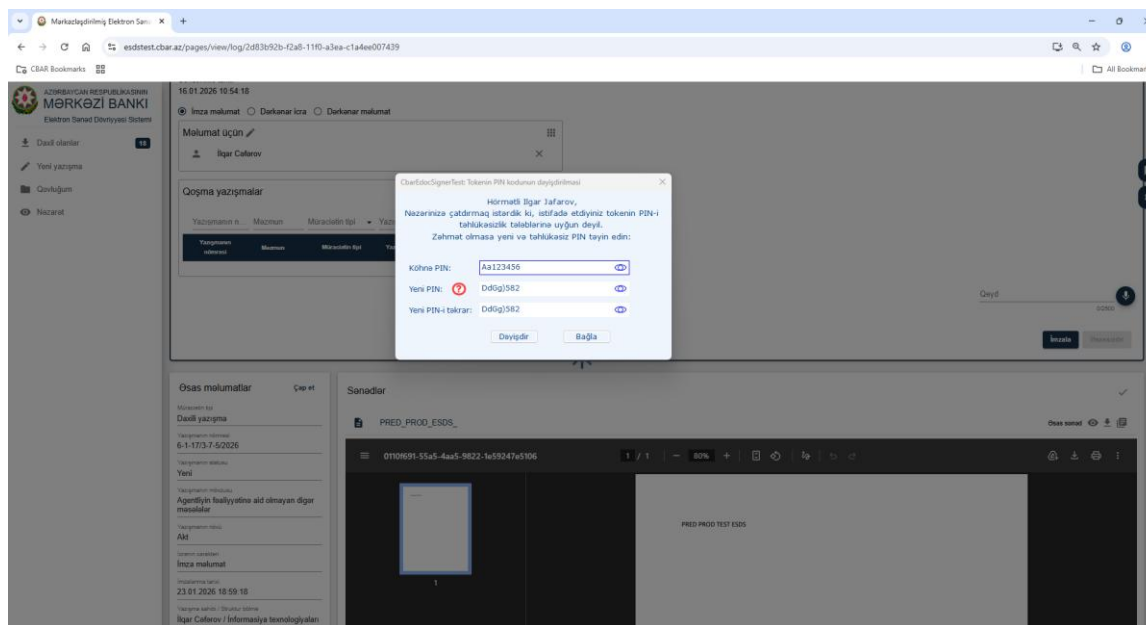
Şəkil 12. “Zəif” PIN kodu ilə imzalama prosesi – Addım 3

PIN kodunun dəyişdirilməsi üçün istifadəçiyə müvafiq interfeys təqdim olunur. İlk olaraq cari PIN kodu, daha sonra təhlükəsizlik tələblərinə uyğun yeni PIN kodu daxil edilir (Şəkil 13).



Şəkil 13. “Zəif” PIN kodunun dəyişdirilməsi

İstifadəçiyə daxil etdiyi yeni PIN kodunu vizual olaraq yoxlamaq imkanı da təqdim olunur (Şəkil 14).



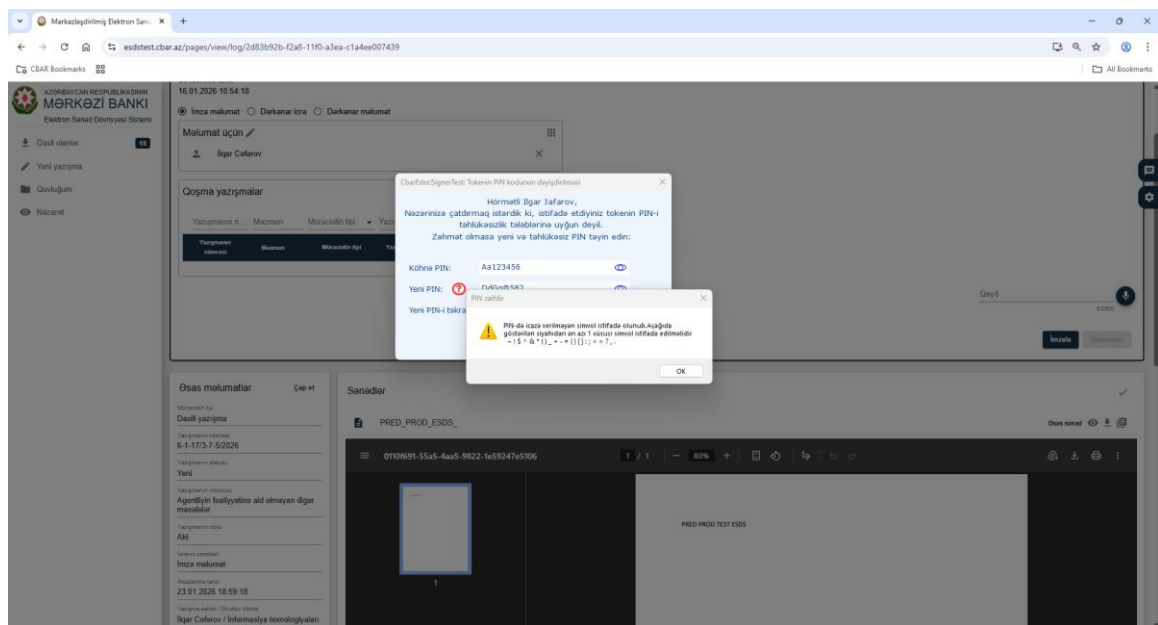
Şəkil 14. PIN kodunun vizual yoxlanılması

İstifadəçi yeni PIN kodunu daxil etdikcə, CbarEdocSigner həmin PIN kodunun müəyyən edilmiş təhlükəsizlik tələblərinə uyğunluğunu yoxlayır.

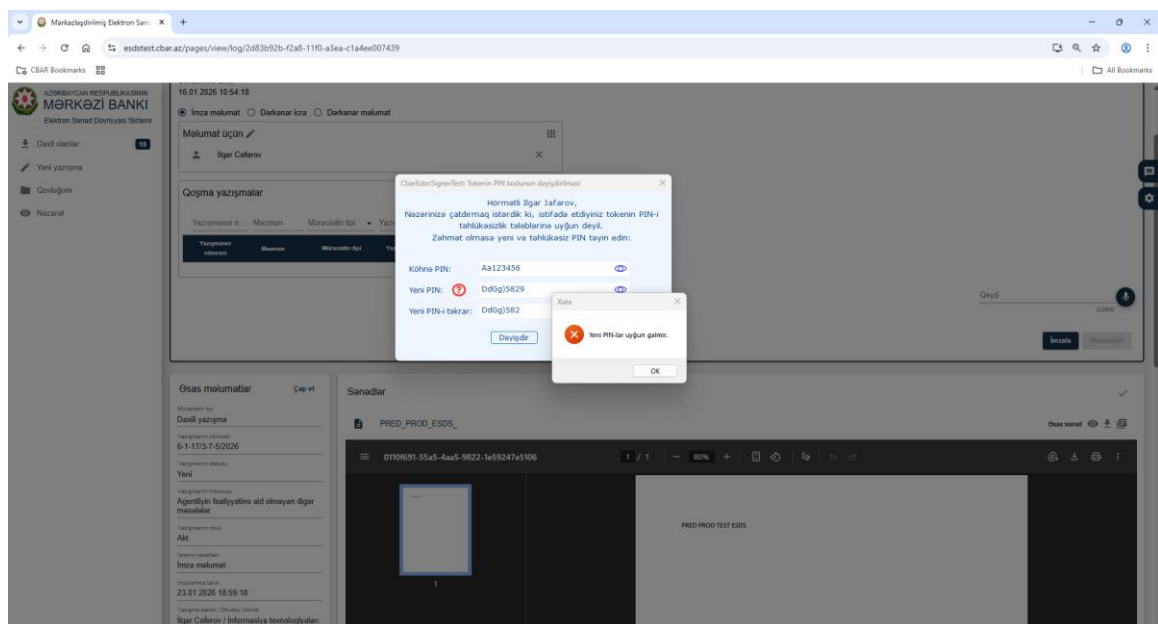
PIN kodunun dəyişdirilməsi prosesi aşağıdakı mərhələlərdən ibarətdir:

- cari PIN kodunun daxil edilməsi;
- yeni PIN kodunun daxil edilməsi;
- yeni PIN kodunun təhlükəsizlik tələblərinə uyğunluğunun yoxlanılması;
- PIN kodunun token üzərində dəyişdirilməsi;
- əməliyyatın nəticəsi barədə istifadəçiyə məlumat verilməsi.

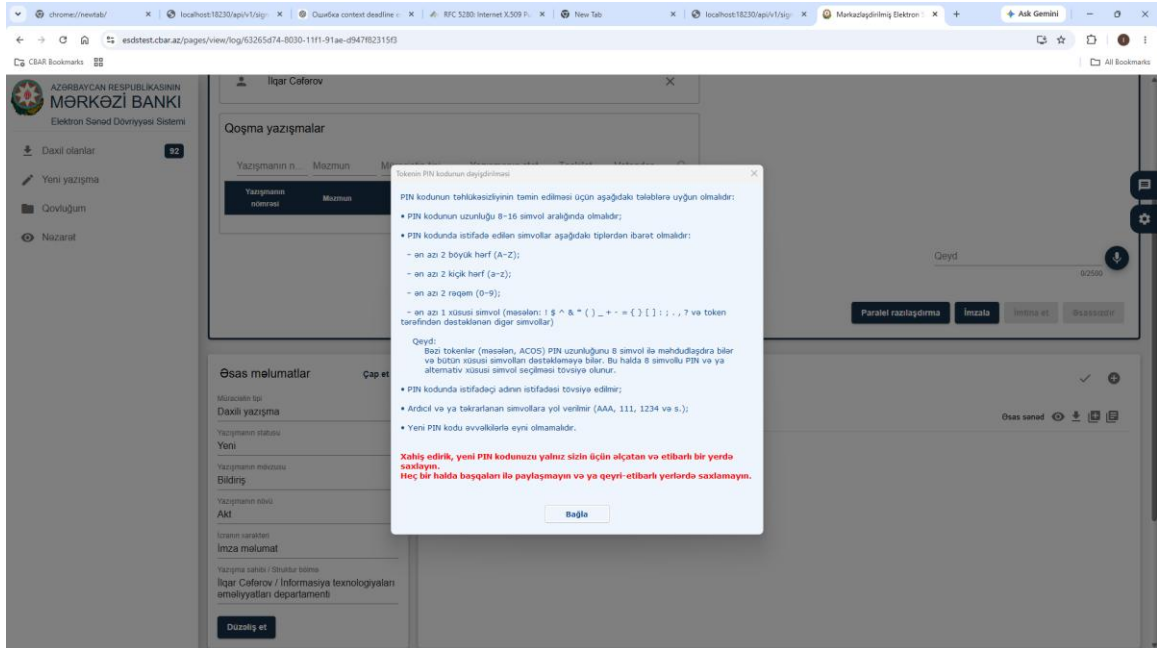
Token ilə aparılan əməliyyatlar üçün məhdud sayda cəhd imkanı mövcuddur. Cəhdlərin maksimal sayı istifadə olunan tokenin modelindən və təhlükəsizlik parametrlərindən asılıdır.



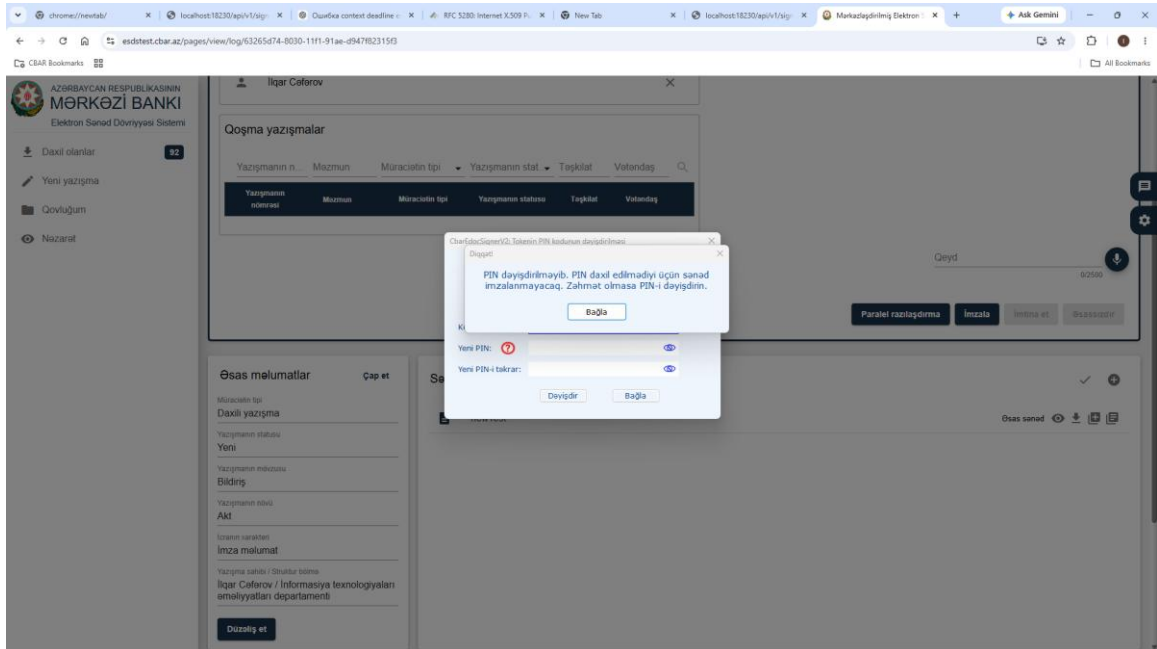
Şəkil 15. PIN kodunun yoxlanılması – Addım 1



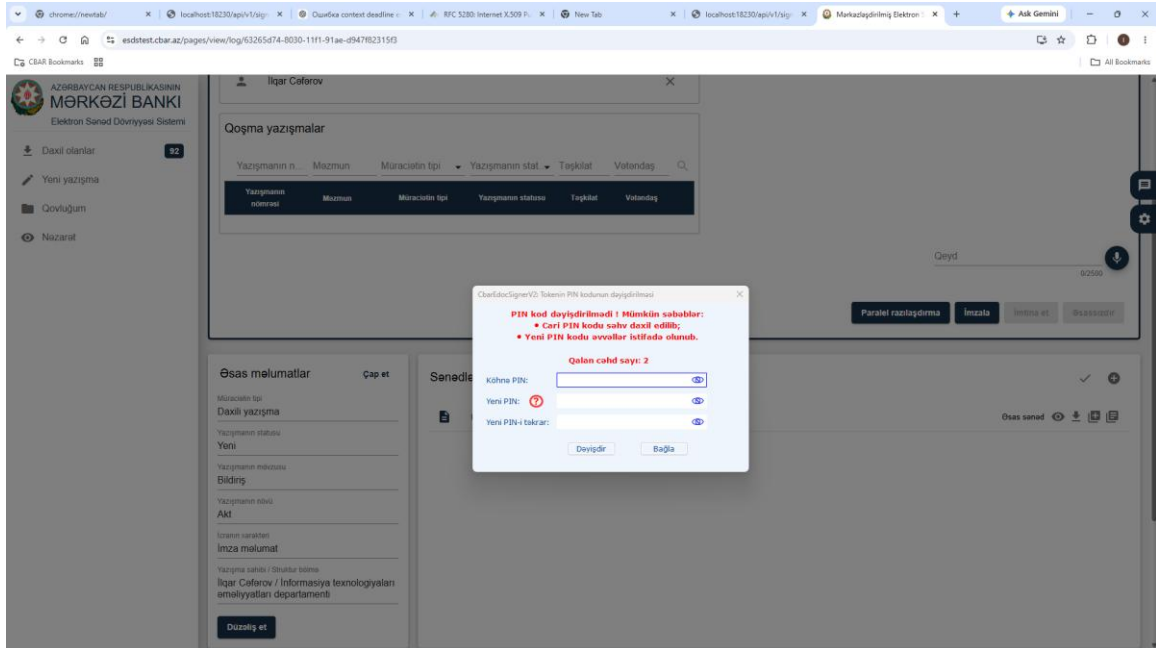
Səkil 16. PIN kodunun yoxlanılması – Addım 2



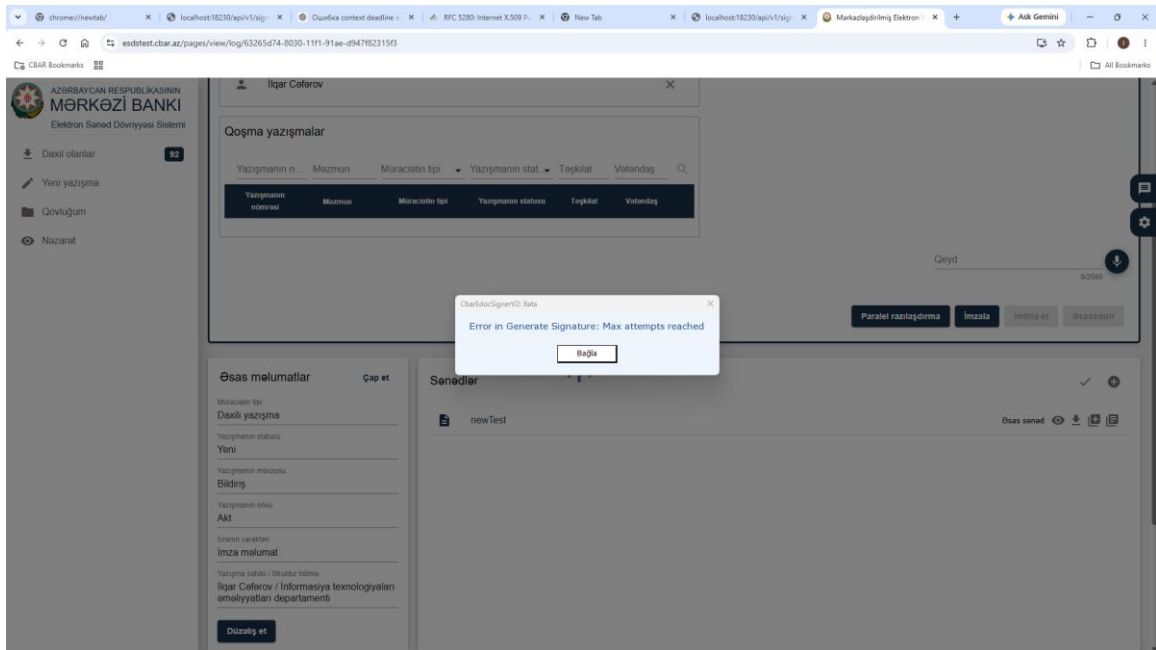
Şəkil 17. PIN kodunun yoxlanılması – Addım 3



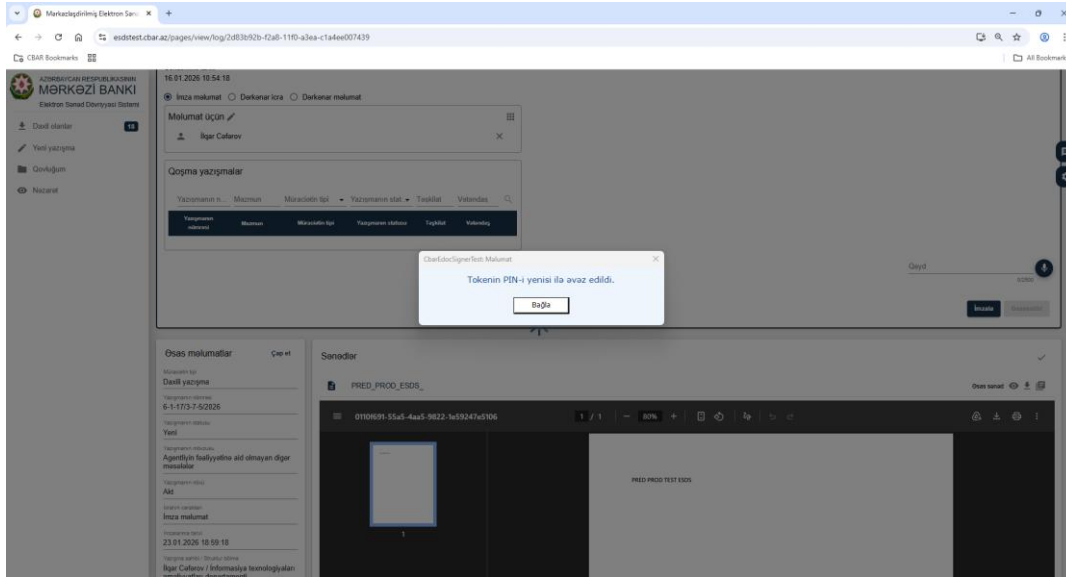
Şəkil 18. PIN kodunun yoxlanılması – Addım 4



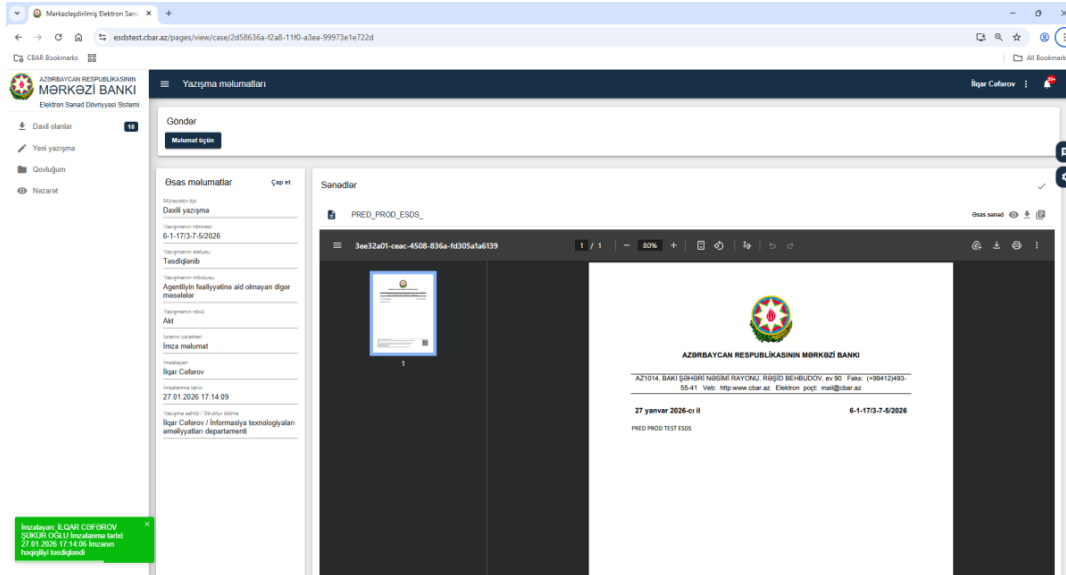
Şəkil 19. PIN kodunun yoxlanılması – Addım 5



Şəkil 20. PIN kodunun yoxlanılması – Addım 6



Şəkil 21. Token PIN kodunun dəyişdirilməsinin uğurla tamamlanması



Şəkil 22. Token PIN kodunun dəyişdirilməsi və imzalama prosesinin tamamlanması