Certificate Login

NRYTN MHM | Azərbaycan, Bakı, Dilarə Əliyeva küç. 185, AZ 1010

TexnİKİ TƏLİMAT

2021

**Təsvir**

Api veb saytlar üçün nəzərdə tutulmuşdur. Məqsədi veb saytlarda elektron imza sertifikatları vasitəsilə autentifikasiya mexanizminin qurulmasıdır.

**Tərkibi**

Api üçün aşağıdakılar zəruridir:

1. Root sertifikatlar kliyent kompüterdə local machine trusted a yazılmalıdır.
2. Driver lər kliyent kompüterə yazılmalıdır.
3. İnteqrasiya olunacaq sistem Milli Sertifikat Xidmətləri Mərkəzində qeydiyyatdan keçməlidir

**1.** **Root sertifikatlar həm serverdə həm kliyent kompüterdə local machine trusted a yazılmalıdır**

1. <http://e-imza.az/downloads/AZ_Root_Authority_(RCA).cer>

2. <http://e-imza.az/downloads/AZ_Policy_Authority_(PCA).cer>

3. http://e-imza.az/downloads/AZ\_Governing\_Bodies\_Authority\_(ICA).cer

4. <http://e-imza.az/downloads/AZ_e-Government_Authority_(ICA).cer>

**2.** **Driver lər kliyent kompüterə yazılmalıdır**

1. <http://e-imza.az/uploads/software/ePass2003-Setup.exe>

2. <http://e-imza.az/downloads/Charismathics%20x64.msi>

3. <http://e-imza.az/downloads/Charismathics%20x32.msi>

**Api üçün istifadə olunan obyektlər**

**Api:**

[https://sxmlogin.e-imza.az:4530/api/v1/certificate/login?origin={Url}](https://sxmlogin.e-imza.az:4530/api/v1/certificate/login?origin=%7bUrl%7d)

**Url:**

İnteqrasiya olunacaq sistemin url-i

(test: https://sxmlogin.e-imza.az:4530/api/v1/certificate/login?origin=http://test.az)

|  |  |  |
| --- | --- | --- |
| Çıxış parametrləri | Tiplər | Qeyd |
| *Output* | string | *Login* prosesinin nəticəsində əldə olunan JWT |
| *IsSuccess* | bool | Api-nin nəticəsinin uğurlu olub olmamasını göstərən parametr |
| *ErrorList* | List<Error> | Api-nin nəticəsinin uğurlu olamadıqda əldə olunan errorlar |

***Error***

|  |  |  |
| --- | --- | --- |
| Detallar | Tiplər | Qeyd |
| *StatusCode* | *int* | Http status kodlar |
| *ErrorCode* | *int* | Apinin error status kodlari |
| *ErrorMessage* | *string* | Apinin error mesajları |

***StatusCode*** *aldığı dəyərlər*

|  |  |  |
| --- | --- | --- |
| Ad | Dəyər (int tipində) | Məlumat |
| *BADREQUEST* | 400 |  |
| *UNAUTHORIZED* | 401 |  |
| *FORBIDDEN* | 403 |  |
| *NOTFOUND* | 404 |  |
| *INTERNAL* | 500 |  |

***ErrorCode*** *aldığı dəyərlər*

|  |  |  |
| --- | --- | --- |
| Ad | Dəyər (int tipində) | Məlumat |
| *INTERNAL\_ERROR* | 1 |  |
| *UNAUTHORIZED* | 2 |  |
| *INPUT\_IS\_NOT\_VALID* | 3 |  |
| *ACCESS\_DENIED* | 4 |  |
| *ORGANIZATION\_DOES\_NOT\_EXIST* | 5 |  |
| *ORIGIN\_IS\_EMPTY* | 6 |  |
| *CLAIMS\_ARE\_EMPTY* | 7 |  |
| *CUSTOMER\_DOES\_NOT\_EXIST* | 8 |  |
| *CUSTOMER\_IS\_BLOCKED* | 9 |  |
| *ORGANIZATION\_IS\_BLOCKED* | 10 |  |
| *SUB\_ORGANIZATION\_IS\_BLOCKED* | 11 |  |
| *CERTIFICATE\_STATUS\_IS\_NOT\_GOOD* | 12 |  |
| *CHAIN\_VALIDATION\_STATUS\_IS\_NOT\_GOOD* | 13 |  |
| *LOGIN\_CERTIFICATE\_VERIFICATION\_IS\_NOT\_GOOD* | 14 |  |

***JWT***

|  |  |  |
| --- | --- | --- |
| Detallar | Tiplər | Dəyəri |
| *cert\_subj\_CN* | *string* | Ad Soyad Ata adı |
| *cert\_subj\_GN* | *string* | Ad |
| *cert\_subj\_SERIALNUMBER* | *string* | Fərdi identifikasiya nömrəsi |
| *cert\_subj\_T* | *string* | Vəzifəsi |
| *cert\_subj\_SN* | *string* | Soyad |
| *cert\_subj\_O* | *string* | Müəssisə |
| *cert\_subj\_OU* | *string* | VÖEN:{vöen}-{sun} |
| *cert\_subj\_C* | *string* | AZ |
| *nameid* | *string* | Fərdi identifikasiya nömrəsi |
| *cert\_validation\_OCSPStatus* | *string* | Good ya Bad |
| *cert\_validation\_OCSPProducedTime* | *DateTime* | *OCSPStatus un yaranma tarixi* |
| *cert\_validation\_Chain* | *bool* | *Chain Validatin nəticəsi* |
| *cert\_VFR* | *DateTime* | Sertifikatın yaranma tarixi |
| *cert\_VTO* | *DateTime* | Sertifikatın bitmə tarixi |
| *nbf* | *int* | JWT nin aktivləşmə tarixi |
| *exp* | *int* | JWT nin bitmə tarixi |
| *iat* | *int* | JWT nin yaranma tarixi |
| *iss* | *string* | JWT ni yaradan mərkəz |
| *aud* | *string* | JWT hansı origin üçün yaradılıb |

[**http://test.az**](http://test.az) **origini üçün test secret key:** Ee+PITxY8kNQ8AD1m56/b6KOL75GVZHLtMWIwNhIaqxaXpPfBCJ/eH5xv624RdIuzJSJdg7mIQl5Pz613ly7dw==

**Secret key** base64 formatındadır. İstifədə olunarkən ByteArray - ə konvertasiya olunmalıdır.

[**http://test.az**](http://test.az) **origini üçün alqoritm:**

http://www.w3.org/2001/04/xmldsig-more#hmac-sha256