ՀՀ քաղաքացիների նույնականացման քարտի միջոցով առցանց իսկորոշման/լիազորման համակարգի հետ ինտեգրման տեխնիկական ձեռնարկ

տարբերակ 1.0

ՀՀ քաղաքացիների նույնականացման քարտի միջոցով առցանց իսկորոշման/լիազորման համակարգը թույլ է տալիս իսկորոշել ինտերնետ օգտատերին օգտագործելով նրա նույնականացման քարտը և տրամադրում է տվյալ քաղաքացու վերաբերյալ անձնական տվյալներ (անուն, ազգանուն, ՀԾՀ) հարցում իրականացնող կազմակերպությանը:

Կազմակերպությունները համապատասխան ծառայությունից օգտվելու համար պետք է ունենան ԷԿԵՆԳ-ի կողմից տրամադրված ինտեգրացման համար անհրաժեշտ պարամետրերը՝ հետքանիշ (token) և ծածկագրման բանալի (secret key):

Հարցումը կատարող կազմակերպությունը իր կայքում (կամ այլ ներքին համակարգում) պետք է համապատասխան հարցում կատարի https://eid.ekeng.am/authorize հասցեին ուղարկելով վերոհիշյալ հետքանիշը և տվյալ օգտատերի սեսիայի համար գեներացված բացառիկ իդենտիֆիկատորը (session ID) որպես մուտքային պարամետրեր:

Տես ներկայացված օրինակը Javascript ծրագրային լեզվի և jQuery գրադարանի օգտագործմամբ՝

```
function authRequestProcess() {

   // Token provided by EKENG
   var token = "6be134a6-07a7-4679-ba0f-96b9fa6c365b";

   // Server side generated user session ID
   var opaque = '1cr8j1po4ejoer6nqm423jdpn3';
   $.ajax({
       type: "POST",
       url: "https://eid.ekeng.am/authorize/",
       data: {
           token: token,
           opaque: opaque
       },
       async: false,
       timeout: 6000,
       dataType: 'json',
       success: function (result) {
           if(result.status == 'OK') {
               alert(result.data);
           }
           else {
               alert("INVALID DATA");
           }

       },
       error: function (xhr, ajaxOptions, thrownError) {
           alert("Please insert your eID card into the reader");
       }
   });
```

```
}
```

Եթե օգտատերի համակարգչի վրա տեղադրված է նույնականացման քարտի աշխատանքի համար անհրաժեշտ ծրագրային ապահովումը, քարտի կարդացող սարքը միացված է համակարգչին և քարտը տեղադրված է կարդացող սարքի մեջ, ապա ծրագրային ապահովումը օգտատերից կպահանջի ներմուծել քարտի PIN համարը վերոհիշյալ հարցումը կատարելու դեպքում:

Օգտվողի ձեռնարկները հասանելի են https://www.ekeng.am/hy/userguide/ հասցեով:

PIN համարի ճիշտ ներմուծման դեպքում սերվերի պատասխանը կունենա հետևյալ JSON ֆորմատի տեսքը՝

```
{"status":"OK","data":"GIme2lVxoSzgzZiIiAo+WNGx+3mibZx5hav3T3KTc
qFzWEYU3HkbvGNfAVUPBbrekj3El2t8Fg0Ly3ygAQWr9aPS0SaJQw+Q5MTlEMpEm
NGIx\/QnyddlccsFK52QTQG7lW2tfZgFdBgq2FcqV7KOzLFhGXrHyibNlPWe8iv\/
Di03GjWWnR8TBxoQiGLp8G5Is2m41OkVFjqIZ7NlMEDLt2HRm6iJuh5BXjexeGcq
3yI="}
```

Օգտատերի ինքնորոշումը համակարգում կատարվում է SSL client certificate-ների միջոցով և քանի դեռ օգտատերը չի ինքնորոշվել իր քարտի միջոցով (քարտը իր մեջ պարունակում է համապատասխան սերտիֆիկատները), ցանկացած հարցում eid.ekeng.am հասցեով կստանա ոչ HTTP 200 պատասխան:

data դաշտը պարունակում է օգտատերի տվյալները կոդավորված OpenSSL AES 256 ալգորիթմով՝ օգտագործելով համապատասխան կազմակերպության ծածկագրման բանալին:
Տվյալ դաշտի պարունակությունը հարկավոր է ապակոդավորել օգտագործելով նույն կոդավորման ալգորիթմը:

Տես օրինակ PHP ծրագրավորման լեզվի օգտագործմամբ՝

```
<?php

// Secret key provided by EKENG
$secret = '4)3jDR4CaWE3I54*k1#W8"[:8C7*k9092V1D`{';
```

```
// Do not change this value
$iv = 'O9fGelU066lJf7tiIjTw7w==';

$user = openssl_decrypt($data, 'aes256', $secret, null,
base64_decode($iv));
if  (!$user) {
    return false;
} else {
    print_r(json_decode($user));
}
```

Ապակոդավորված տվյալները իրենցից ներկայացնում են JSON տիպի տվյալներ ներքոհիշյալ պարամետրերով՝

Պարամետրի անվանում	Նկարագրություն	Տվյալի տիպ
opaque	Կազմակերպության կողմից ուղարկված և նույնապես հետ ստացված պարամետր	String
last_name	Ազգանուն	String
first_name	Անուն	String
SSN	Հանրային ծառայության համար	Intager (10)

Պարտադիր պայման է հանդիսանում պատասխանի մեջ ստացված “opaque” պարամետրի ստուգումը կազմակերպության կողմից ուղարկված և պահպանված պարամետրի հետ:

Հարցմանը ի պատասխան կարող են ստացվել նաև հետևյալ տիպի հաղորդագրություններ՝

```
{"status":"forbidden","message":"ERROR message here"}
```

Սխալ	Պատճառ
Request token or opaque parameter missing	Մուտքային պարտադիր պարամետրերը ներկայացված չեն
Request token isn't correct	Ուղարկված հետքանիշը ճիշտ չէ
Token expired	Տրամադրված հետքանիշի գործողության ժամկետը սպառված է

Տվյալ համակարգը, ելնելով նույնականացման քարտի հետ աշխատելու համար անհրաժեշտ Cryptocard Suite Manager ծրագրայի փաթեթի առկա սահմանափակումներից, այս պահին աշխատում է միայն Windows ընտանիքի օպերացիոն համակարգերով համակարգիչների համար, Google Chrome և Opera զննարկիչներում:

Խորհուրդ է տրվում դրա մասին համապատասխան նշում կատարել ինտեգրվող կազմակերպության էջում: