Yeni nəsil şəxsiyyət vəsiqələrinin (E-ID) e-xidmətlərə inteqrasiyası problemləri

Həbib Abbasov
AR Nəqliyyat, Rabitə və Yüksək Texnologiyalar Nazirliyi
AMEA İnformasiya Texnologiyaları İnistutu, Bakı, Azərbaycan
hebib.atilla@gmail.com

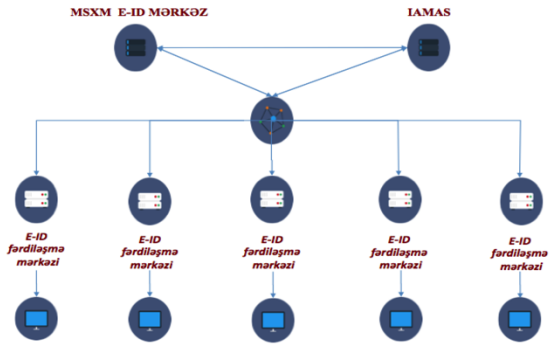
Xülasə — Müasir dövrdə informasiya texnologiyalarının inkişafı dövlətlərdə və hökümətlərdə ənənəvi klassik xidmətlərin elektron xidmətlərə keçidinə zəmin yaratmışdır. Bu isə öz növbəsində hər birimizin daxil olduğu informasiya cəmiyyətində, vətəndaşlara məxsus fərdi məlumatların etibarlı qorunması və təqdim olunan, yeni nəsil şəxsiyyəti təsdiq edən sənədin elektron çip daşıyıcısı vasitəsi ilə informasiya təhlükəsizliyi amilini daima qüvvədə saxlayır.

Yeni nəsil şəxsiyyət vəsiqəsi (e-İD) informasiya mübadiləsində beynəlxalq mülki aviyasiya təşkilatı (İCAO) tərəfindən təklif olunmuş bütün texniki və texnoloji tələbləri özündə əks etdirir. Bu tələblər əsasında vətəndaşlara yeni nəsil nəsil şəxsiyyət vəsiqələrinin verilməsi üçün Azərbaycan Respublikası Prezidenti 2014-cü il 28 noyabr tarixli 893 nömrəli sərəncam[1] imzalamışdır. Sərəncamdan irəli gələn məsələlər içərisində e-xidmətlərə əlçatanlığın təmin edilməsi üçün hər bir imza səlahiyyəti olan vətəndaşa elektron imza sertifikatları verilməsi göstərilmişdir. E-İD həllərində elektron imzanın (e-imza) tətbiqi e-sənəd, elektron bankaçılıq, qorunan e-poçt, e-səhiyyə, portal və bulud üzərində e-xidmətlərin təhlükəsizliyinin təmin edilməsində mühüm yer tutur. Məqalə tətbiq olunan yeni nəsil şəxsiyyət vəsiqələrinin kriptoqrafik imkanları əsasında e-imza sertifikatları istifadəsi eyni zamanda ümumi istifadə üçün açıq olan vəsiqə məlumatlarının çipdən oxunması və elektron xidmətlərə inteqrasiyada qarşıda duran problemlərə həsr olunmuşdur.

Açar sözlər— e-gov; e-imza; e-İD; e-sənəd; CSP, ECC, SHA-2

1. GİRİŞ

E-İD smart kartlar texniki olaraq xülasədə də qeyd olunduğu kimi müəyyən olunmuş tələblərə əsasən formalaşdırılmışdır. Bu tələblər əsasında təqdim edilən e-İD kartlar özündə bir çox məlumatların saxlanılması təmin edir. E-İD kartların 2018 –ci il 1 sentiyabr tarixdən verilməsi prosesi başlanmışdır. Ölkə üzrə regionlarda mərkəzləşdirilmiş qaydada e-İD kartların verilməsi üçün fərdiləşmə mərkəzləri qurulmuşdur. Qurulmuş mərkəzlərə daxil olunmuş müraciətlər əsasında vəsiqələrin İAMAS sisteminə qoşulmaqla hazırlanması prossesi icra edilir. Hər bir fərdiləşmə mərkəzi üzrə müraciət əsasında Milli Sertifikat Xidmətləri Mərkəzinə vətəndaşa aid olan ərizə məlumatı və PKCS#7[2] formatında sertifikat sorğusu göndərilir. Sorğuların dəqiqliyinin təmin edilməsi üçün MSXM tərəfindən fərdiləşmə mərkəzlərnə xüsusi olaraq infrsatruktur sertifikatları verilmişdir. Bu sertifikatlar vasitəsi ilə informasiya mübadiləsində ötürülən məlumatların səhihliyinin və məlumatın ötürmə mənbəyinin identikləşdirilməsi təmin edilir. Şəkil 1-dəki blok sxemdə e-İD sertifikat xidmətləri mərkəzi ilə İAMAS və regionlar üzrə fərdiləşmə mərkəzlərinin qoşulma sxemi təsvir edilmişdir.



Şəkil 1 E-İD mərkəz ilə İAMAS və fərdiləşmə mərkəzləri arasında struktur sxemin təsviri

II. HƏLLİN TƏTBİQİ VƏ AÇARLARIN SAXLANMA VASİTƏLƏRİ

Hal-hazırda Azərbaycan Respublikasında e-imza sertifikatlarının verildiyi yeni nəsil şəxsiyyət vəsiqəsi üçün istifadə edilən smart kart çipinin daxilindəki açarların təhlükəsizliyi aşağıda göstərilən tələblərə cavab verir.

GEMALTO NXP P60D144[3]
ISO 7816 – 4,8,9,15 standard, T=1, T=0 protocol, 384-Kbyte ROM, 8.125 -Kbytes RAM, 144-Kbyte EEPROM, Asymmetric – RSA, ECC algorithm, symmetric – Triple DES, DES, AES hash SHA2, CC EAL5+ certified, Supports PC/SC/ PKCS11/ CT-API

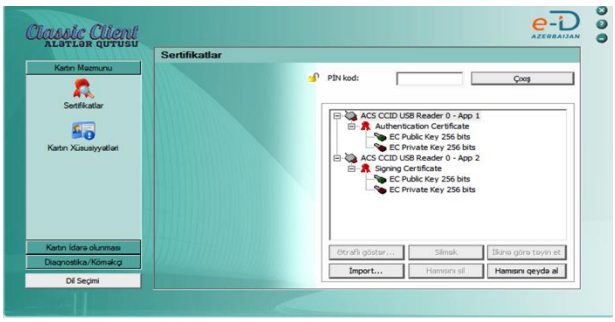
Smart kartın konteynerləri imzalama və həmçinin şifrələmə funksiyalarına malikdir.

Kriptoqrafiq xarakteristikalar ümumilikdə beynəlxalq standartlar əsasında qurulub. E-İD kartlar aşağıda qeyd olunan kriptoqrafiq servis (CSP) vasitəsi ilə e-imza sertifikatlarına icazəni təmin edir.

İnformasiya təhlükəsizliyi baxımından əsas olan milli problem kimi smart karların təhlükəsizlik kompanenti kimi

DOI: 10.25045/NCInfoSec.2018.17

istifadəsində CSP və təsadüfi açar generasiyası funksiyasının (RNG) milli olmamasıdır. Aşağıdakı təsvirdə e-İD kartlarında e-imza sertifikatları vasitəsi ilə sənədlərin imzalanması üçün aralıq interfeys proqram təminatı əks olunub.



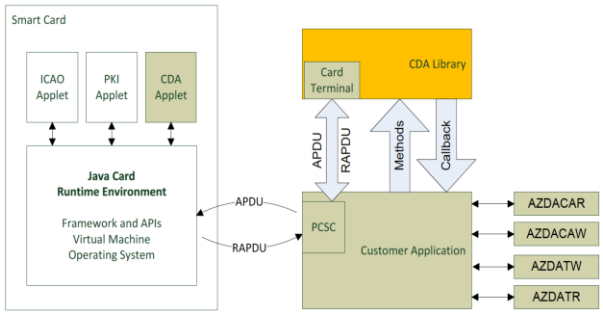
Şəkil 2 E-İD kartlarında olan açarların və sertifikatların oxunması üçün təqdim olunan proqramın təsviri

Proqram təminatı istehsalçı tərəfindən dörd əməliyyat sistemi üçün təqdim edilib.

1. Windows
2. Linux
3. Mac OS
4. Android

Təqdim olunan e-İD kartlar bir çox ölkələr üzrə müqayisədə istehsalçıdan müəyyən asılılığın olması ilə fərqlənir. Bu isə kartlardan istifadədə misal olaraq İOS əməliyyat sistemi üçün mümkün deyil. PKCS#11 standartı üzrə APDU müraciət etdikdə istehsalçı tərəfindən xüsusi “Master Key” ilə PKCS#11 müraciəti şifrələnməsi təmin edilmişdir. Türkiyə, Avstriya, İtaliya təcürbəsinə baxdıqda bu tip həllər hər bir proqramist üçün açıqdır. Bu isə e-İD kartlar üçün formalaşdırılan bütün e-xidmətlər üçün açıqdır. Bura daxildir veb, mobil, blud həllər üzrə formalaşdırılan elektron xidmətlər.

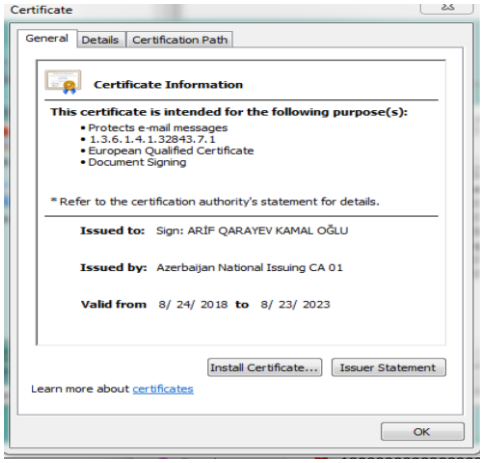
Hal –hazırda təqdim edilən e-İD kartlar aşağıda göstərilən göstərilən apletlər ilə təmin edilib.



Şəkil 3 E-İD kartlarında təqdim olunan apletlərin təsviri

1. İCAO aplet beynəlxalq mülki aviyasiya təşkilatının tələb etdiyi məlumatları özündə əks elətdrir. Bura daxildir, vəsiqə sahibinin foto şəkli, verilmə tarixi, verən orqanın adı. Bu məlumatların əldə edilməsi ancaq NFC texnologiyası ilə "Basic Access Control" BAC[4] metodu ilə mümkündür.
2. PKİ aplet e-imza sertifikatlarının saxlanılması üçün istifadə edilir. PKİ aplet şəkil 2 - də təsvir edilmiş açarları və sertifikatları özündə saxlayır. Apletdə bir cüt sertifikat saxlamaq imkanı mövcuddur. Qanunvericiliyə uyğun olaraq yaş həddinə görə sertifikatlar MSXM tərəfindən e-İD vəsiqələrin çipinə daxil edilir. Yaş həddi 10-15 olan vətəndaşlar üçün ancaq bir autentifikasiya sertifikatı təqdim edilir. Bu sertifikat vasitəsi ilə təqdim edilən və gələcəkdə təsvir ediləcək istənilən e-gov xidmətlərinə identifikasiya olunması nəzərdə tutulub. Yaş həddi 15 dən yüxarı olan vətəndaşlar üçün iki sertifikat mərkəz tərəfindən PKİ apletə yazılır. Bunlar imza və autentifikasiya sertifikatlarıdır. Sertifikatların yaşam müddəti 5 ildir. E-İD vəsiqənin etibarlılıq müddəti isə 10 il nəzərdə tutulub. Hər 5 ildən bir istifadəçilər sertifikatlarının yenilənməsi üçün müvafiq mərkəzlərə müraciət edəcəklər.

Sertifikatlar ellptik əyrilərə əsaslanan kriptoqrafiq algoritmlərlə təmin edilib. ECDH_P256 bit uzunluğa malikdir. SHA384 heş funksiya ilə heşləmə əməliyyatları icra edir. Aşağıdakı təsvirdə vətəndaşa verilmiş imza sertifikatı əks olunub.

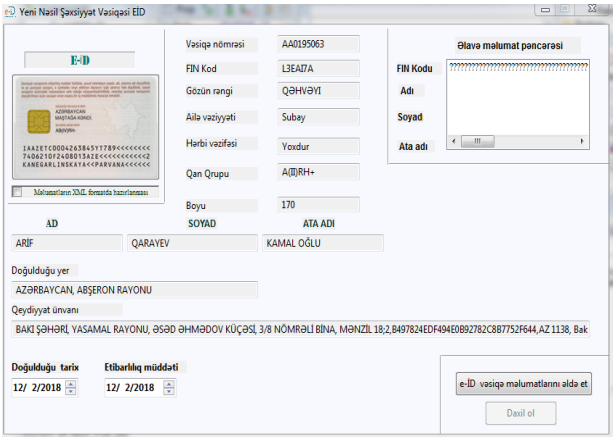


Şəkil 4 E-İD kartlarda vətəndaşlara təqdim olunan imza sertifikatının təsviri

Sertifikatlar avropa directivinin[5] 2014 –cü ildə qəbul etdiyi tələblər əsasında formalaşdırılıb.

3. CDA apleti şəxsiyyət vəsiqəsi formalaşadırılması üçün fərdə məxsus informasiyaları özündə saxlayır. Bu hissədə dəyişə bilən və dəyişməyən məlumatlar yerləşdirilmişdir. Dəyişə bilinən məlumatlar ancaq xüsusi sertifikatla müvafiq icra hakimiyyəti orqanına məxsusdur. Misal olaraq vətəndaşın ünvanı dəyişdikdə onun yenidən e-İD kart almasına ehtiyac olmur. Bu dəyişə bilinən məlumat olduğundan müvafiq qrumda e-İD kart oxuyucuya daxil edilməklə dəyişdirilir.

Elektron xidmətlərə inteqrasiyada bu sahədə müəyyən problemlər movcuddur. Əsasən vətəndaşların bankalara və özəl təşkilatlara müraciəti zamanı vəsiqələrdən məlumatların oxunması problemi ilə qarşılaşırlar. Bu problemin aradan qaldırılması üçün aşağıda təsvir olunan proqram təminatı tərəfimizdən formalaşdırılmışdır.

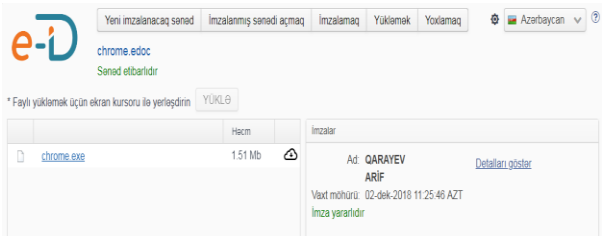


Şəkil 5 E-İD kartlarda vətəndaşlara məxsus olunan məlumatların oxunması proqramının təsviri

III. E-ID VƏ E-İMZA TƏTBİQİNDƏ ETİBARLI XİDMƏTLƏR

Avropa birliyi ölkələri müvafiq qanunvericiliklərində bir çox ənənəvi xidmətlərin elektronlaşması üçün təkmilləşdirmə aparıblar. Bu qanunvericilik ümumilikdə eİDAS[6] adlanır. eİDAS qanunvericiliyi birlik ölkələri arasında etibarlı e-xidmətlərin formalaşmasını və e-imzaların qarşılıqlı tanınması mexanizmini hüquqi müstəvidə müəyyən edir. Hal-hazırda “e-imza və e-sənəd” haqqında qanunun optimallaşması və gələcək çağrışlara cavab verməsi vacibdir. Bu baxımdan etibarlı e-xidmətlər göstərilən zaman tərəflərin tanınması texniki və hüquqi baxımdan tam olmalıdır. Ancaq təcrübələr göstərir ki, texnoloji inkişaf qanunvericilikləri qabaqlayır.

E-imzalar vasitəsi ilə hal-hazırda bir cox xidmətlərə çıxış imkanları təmin edilib. E-İD kartlarda təqdim edilən imza sertifikatları kriptoqrafiq alqoritm baxımından carı istifadədə olan e-imzalardan fərqləndiyi üçün formalaşdırılan e-sənəd tipləri müxtəlif olacaq. Bu isə ilk növbədə inteqrasiya mərhələlərində bir çox təşkilatı və resurs problemləri ilə özünü göstərəcək. Hal-hazırda tətbiq edilən e-sənəd formatları edoc genişlənməsində olub CADES formatında icra edilir. E-İD platforması üzrə tədim edilən sənəd yaratma formatı ETSI EN 319 162 Associated Signature Containers (**ASiC**)[7] formatıdır. Aşağıda qeyd olunan təsvir nümunəsində e-İD kartlarda təqdim edilən e-imzalar vasitəsi ilə e-sənədlərə imza əlavə edilməsi üçün veb üzərindən təqdim edilən proqram təminatı əks olunmuşdur.



Şəkil E-İD kartlarda vətəndaşlara təqdim olunan imza sertifikatı ilə sənədlərin imzalanmasının təsviri

NƏTİCƏ

E-dövlət quruculuğunda informasiyanın qorunması və onun təhlükəsizliyinə təhdidlər genişlənir. Milli informasiya təhlükəsizliyin təmin edilməsi baxımından yeni e-İD kartların tətbiqi müsbət amildir. Ancaq yuxarıda qeyd etdiyim bir çox kriptoloji və texniki təşkilatı yanaşmalar dahada təkmilləşdirilməlidir. Tətbiq olunan həllin milli riyazi və texnoloji həllər olması vacibdir. Bütün bu həllərin ümumistifadə üçün mobil platformalara soft həllər kimi inteqrasiya edilməsi və e-xidmətlərin dayanıqlılığı üçün blud həllərin genişlənməsi məqsədəuyğundur.

ƏDƏBİYYAT

[1] http://www.e-qanun.az/framework/28818
[2] https://en.wikipedia.org/wiki/PKCS
[3] https://www.commoncriteriaportal.org/files/epfiles/0840b_pdf.pdf
[4] https://pdfs.semanticscholar.org/f479/eb98a06a2ed74e67a48acc13ea0237d168d1.pdf
[5] https://europa.eu/european-union/eu-law/legal-acts_en
[6] https://ec.europa.eu/digital-single-market/en/trust-services-and-eid
[7] https://comserv.cs.ut.ee/home/files/Nugis_CyberSecurity_2018.pdf?study=ATILoputoo&reference=F167B647D3821CD1F14EE4922D0E26A9D256FF5B

PROBLEMS OF INTEGRATING NEW GENERATION ID CARDS (E-ID) INTO E-SERVICES

Habib Abbasov
AR Ministry of Transport, Communication and High Technologies
Institute of Information Technology of ANAS
hebib.atilla@gmail.com

Abstract -Order of the President of the Republic of Azerbaijan No 893 of 28 November 2014 implies issuing new generation ID cards to citizens and the order is already being implemented. The order envisages granting e-signature certificates to each signatory citizen to ensure access to e-services. E-signature application for E-ID solutions is essential to ensure the e-security, e-banking, e-mail, e-health, portal and cloud e-services. The article is devoted to the problems encountered in integrating e-ID into e-services.

Keywords - e-Gov; e-signature; e-ID; e-document; CSP, ECC, SHA-2