E-hökumət həllərində mobil imza texnologiyaları

Həbib Abbasov

Azərbaycan Respublikası Rabitə və Yüksək Texnologiyalar Nazirliyi, Məlumat Hesablama Mərkəzi
hebib@rabita.az

***Xülasə*— Müasir dövürdə informasiya texnologiyalarının inkişafı hər birimizin daxil olduğu informasiya cəmiyyətində, informasiya təhlükəsizliyi amili daim öz aktuallığını saxlayır. Mobil həllər sırasında elektron imzanın (e-imza) tətbiqi e-sənəd, e-bankaçılıq, təhlükəsiz e-poçt, portal və bulud üzərində e-xidmətlərin təhlükəsizliyinin təmin edilməsində mühüm yer tutur. E–imza alqoritmlərinin məhdud resurslu mobil qurğularda tələb olunan standartlara uyğun olaraq (bura PKCS#7,CMS, XAdES, CAdES, PAdES e-imza standartları da daxildir) smart kart vasitəsi ilə elektron sənədlərin imzalanması təmin edilməsi tədqiqatlar əsasında aparılmalıdır. Məqalə kriptoqrafik əsaslı smart kartların köməyi ilə Android tipli smartfonlarda gücləndirilmiş elektron imzanın formalaşmasını təmin edən proqram təminatının hazırlanmasına və aparılan tədqiqatlarda əldə edilmiş nəticələrin müqayisəsinə həsr olunmuşdur.**

Açar sözlər*— *e-gov; e-imza; m-imza; e-sənəd; CSP, CA, RSA, SHA-1.

I. GİRİŞ

İnformasiya mübadiləsində ötürülən məlumatların səhihliyinin və məlumatın ötürmə mənbəyinin identikləşdirilməsi informasiya təhlükəsizliyinin əsas sütunlarından biridir. İnformasiya cəmiyyətinin sürətlə formalaşdığı bir mühitdə e-hökumət (e-gov) həllərinin təhlükəsizliyinin təşkili vacib olan amillərdən biridir. Avropa Birliyinin bu sahədə qəbul etdiyi Direktivə [1] əsasən Birliyə daxil olan ölkələr həmin standartlar əsasında işlərə başlamışdılar. Avstriya təcrübəsinə nəzər saldıqda hər bir vətəndaşın yeni nəsil şəxsiyyət vəsiqəsində (eİD kartında) elektron imzaların formalaşmasını təmin edən açarlar və sertifikatlar daxil edilmişdir. Qeyd edildiyi kimi, e-sənədlərin imzasının formalaşmasında e-imza və ya mobil imzadan (m-imza) istifadə etməklə müxtəlif imza formatlarının tətbiqi reallaşdırılır. Bu formatlar XMLsig [2] PKCS#7 və AdES ailəsinə daxil olan XADES, PADES, CADES formatlarıdır.

II. HƏLLİN SEÇİLMƏSİ VƏ AÇARLARIN SAXLANMA VASİTƏLƏRİ

Məlumdur ki, imza yaratma (gizli açar) və imza yoxlama məlumatları (açıq açar) müxtəlif formalarda saxlana bilər. Vacib olan əsas məsələ odur ki, seçilən həll üzrə gizli açarın təhlükəsizliyi tam təmin edilə bilinsin və CSP (Kriptoqrafiya Xidmətinin Təchizatçısı) müxtəlif əməliyyat sistemləri üçün açarlardan və sertifikatdan istifadəni təmin edə bilsin. Açarlar iki vasitə ilə qoruna bilir: proqram təminatı və ya aparat təhlükəsizlik modulların vasitəsilə. Proqram təminatı vəsitəsi ilə təmin edilən açarların təhlükəsizliyik səviyyəsi qəbul edilməz qədər aşağıdır və mobil quğularda sənədlərin imzalanması üçün yararsızdır [3]. Bu amil əsas gətirilərək beynəlxalq təcrübədə ciddi sistemlərdə istifadə edilmir.

Aparat modulları əsasında açarların qorunması 3 növ formada təşkil olunur [4]:

- Smart kartlar,
- Smart kart tipli USB tokenlər,
- Aparat təhlükəsizlik modulları (ing. HSM − Hardware Security Module).

CƏDVƏL 1. Açarların saxlanma sistemləri

№	Meyar	Smart kart	HSM
1	Sertifikatlaşdırma: FIPS 140-2 Level 3	Xeyr	Bəli
2	Qurğuda açarların generasiyası	Bəli	Bəli
3	Açarların nüsxələnməsi	Xeyr	Bəli
4	Müxtəlif imkanlı autentifikasiya	Bəli	Bəli
5	Sürət	Zəif	Sürətli
6	Rolların bölünməsi	Xeyr	Bəli
7	Avtomatikliyi	Xeyr	Bəli
8	Məhv edilməsi	Bəli	Bəli

Hazırda Azərbaycan Respublikasında e-imza üçün istifadə edilən smart kart çipinin daxilindəki açarların təhlükəsizliyi aşağıda göstərilən cədvəl 2-yə uyğundur [5].

CƏDVƏL 2. Siemens CardOS 4.4

ID-1 size, ISO 7816 – 4,8,9 standard, T=1 protocol,
Processor SLE 66CX680PE 8/16 bit security controller,
244-Kbyte ROM, 7100 bytes RAM, 68-Kbyte EEPROM, Asymmetric - RSA 2048 bit algorithm, symmetric – Triple DES, DES, hash SHA1, CC EAL5+ certified,
supports PC/SC/ PKCS11/ CT-API

Smart kartın konteynerləri imzalama və həmçinin şifrələmə funksiyalarına malikdir.

CƏDVƏL 3. Gemalto MultiApp ID 72k Java card

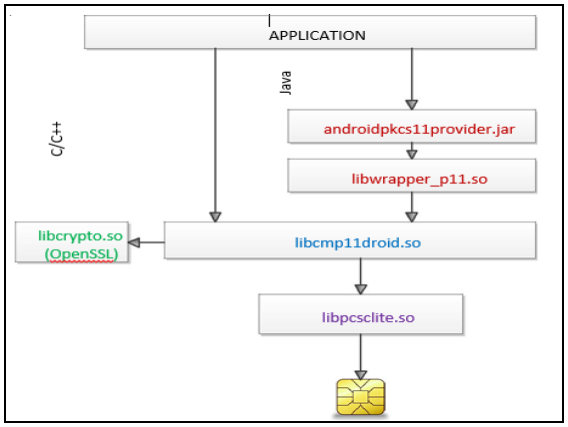
JavaCard Virtual Machine, RTE and API COMPLIANT with JC2.2.1, EEPROM 72K
Cryptographic algorithms: 3DES (ECB, CBC), RSA up to 2048bit
SHA-1, Multiple Logical Channel (permit selection of multiple applets at the same time), Interface T=0 & T=1, FIPS 140,
CC EAL4+ certification

Açarların saxlanıb qorunması vasitələrinə görə təcrübədə mobil imzanı bir neçə üsulla əldə etmək mümkündür [6]. Qəbul edilən mobil imza həllərində əsas funksiyanı mobil operator və sertifikat mərkəzi (Certificate Authority, CA) yerinə yetirirlər. İmza sahibi gizli açarına müraciət etdikdə hər dəfə SMS vasitəsi ilə sertifikat mərkəzinin açarları qoruyan aparat təhlükəsizlik moduluna müraciət etməsi nəticəsində serverin köməkliyi ilə elektron sənədin elektron imzası yaradılır. Lakin imza sahibinin nəzarəti altında yaradılmayan e-imza gücləndirilmiş imza kimi qəbul edilmir.

Qeyd edilən problemin Android tipli smartfonlarda aradan qaldırılması məqsədilə RSA 2048-bit şifrləmə alqoritmi əsasında zəruri e-imza proqram təminatı Java Eclipse proqramlama mühitində yazılmışdır. Mobil imzanın smart-fonda yaradılması üçün gizli və açıq açarlarla bərabər autentifikasiya və imza sertifikatları olan smart kart, mobil kart oxuyucusu və həmçinin mobil qurğunun özünün texniki imkanları və əməliyyat sistemi istifadə edilmişdir (şəkil 1).

Şəkil 1 Mobil e-imza proqramının android smartfonda təsviri

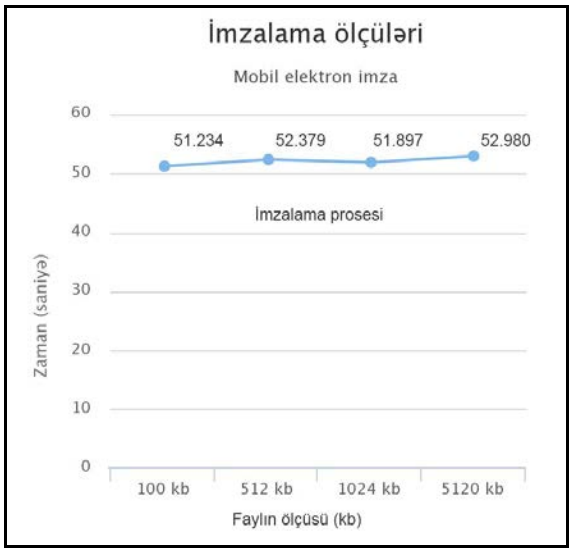
Proqram təminatı SHA-1 heş alqoritmini dəstəkləyir.




```
import org.opensc.R;
import org.opensc.pkcs11.PKCS11Provider;

import android.app.Activity;
import android.os.Bundle;
import android.util.Log;

public class TestActivity extends Activity {
    private final String TAG = TestActivity.this.getLocalClassName();

    static {
        System.loadLibrary("wrapper_p11");
        System.loadLibrary("pcsclite");
        System.loadLibrary("crypto");
        System.loadLibrary("ssl");
    }

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        try {
            PKCS11Provider provider = new PKCS11Provider(this,
                    R.raw.libcmp11droid);
            // Business logic

            provider.cleanup();
        } catch (IOException e) {
            Log.e(TAG, e.getMessage());
            e.printStackTrace();
        }
        super.onCreate(savedInstanceState);
    }
}
```

Şəkil 2 PKCS#11 interfeysin blok sxemi və kitabxanaların yükləyən modulunun təsviri

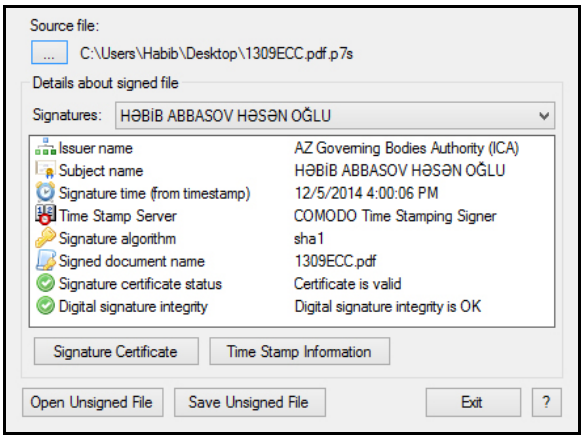
Şəkil 2-dəki blok sxemdə mikroprosessor əsaslı smart kartla proqram arasında məlumat mübadiləsini təmin edən PKCS#11 interfeysin təsviri verilmişdir. Funksional kitabxanalar yüklənildikdən sonra smartfondan smart kart daxilində yerləşənməlumatları eldə etmiş oluruq.



Şəkil 3 İmzalama müddətinin fayl uzunluğundan asıllılığı

Android tipli smartfonlarda imzalama müddətinin elektron sənədin müxtəlif uzunluqlarından asılılığı Şəkil 3-də təqdim edilir. Beləliklə, şəkildən imzalama müddətinin faylın həcmindən asıllılığının olmadığını müşahidə edirik. Əslində

belə bir nəticənin əldə edilməsi gözlənilməndir, çünki elektron imzanın yaradılmasında istifadə edilən SHA1 (160 bit) xeş funksiyanın hesablama müddəti faylın uzunluğundan asılı deyil.



Şəkil 4 PKCS#7 formatda imzalanmış sənədin təsviri

Bu proqram təminatı üzrə sənədlərin imzalanmasında avadanlıqların məhdud resurslarını nəzərə alaraq PKCS#7 standartına uyğun p7s formatında (Şəkil 4) e-sənədi yaradır. İmzalama zamani smart kartın daxilindəki sertifikatlar OCSP servisi vasitəsi ilə RYTN-in Milli Sertifikat Xidmətləri Mərkəzinin bazası ilə yoxlanılır, eyni zamanda E-sənədə həmin sertifikat daxil edilir. Həmçinin imzalama prosesində elektron sənədə vaxt göstəricisi də (TimeStamp) əlavə edilir.

MİNNƏTDARLIQ

Eksperimentlərin aparılmasında yaradılan şəraitə görə Rabitə və Yüksək Texnologiyalar Nazirliyinin Məlumat Hesablama Mərkəzinin direktoru cənab N. Mərdanova və müzakirələrdə verilən ətraflı məsləhətlərə görə Milli Sertifikat Xidmətləri Mərkəzinin müdiri cənab A. Mailiova təşəkkürlərimi bildirirəm.

ƏDƏBİYYAT

[1] European Union: Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Official Journal of the European Communities, 1999.

[2] D. Eastlake, J. Reagle, D. Solo, XML Signature Syntax and Processing. 2nd ed., W3C Recommendation, http://www.w3.org/TR/xmldsig-core/.

[3] http://en.wikipedia.org/wiki/PKCS_12

[4] M. Sarrel, " IronKey USB Flash Drives Prove Their Mettle, 2010. http://www.eweek.com/c/a/Data-Storage/IronKey-USB-Flash-Drives-ProveTheir-Mettle-718976/

[5] Charismathics Smart Security Interface V 4.9. Manual. https://www.charismathics.com/fileadmin/files/pdf/manuals/CSSI_49_EN.pdf

[6] T.Zefferer, A.Tauber, B. Zwattendorfer, K. Stranacher, "Qualified PDF signatures on mobile phones," Electronic Government and Electronic Participation - Joint Proceedings of Ongoing Research and Projects of IFIP EGOV and IFIP ePart, pp. 115-123, 2012.