Crypto Usbtoken və Smartsd-də E-imzanın Tətbiqi

Həbib Abbasov
AMEA İnformasiya Texnologiyaları İnistutu, Bakı, Azərbaycan
hebib@rambler.ru

***Xülasə* — Müasir dövrdə informasiya texnalogiyalarının inkişafı informasiya təhlükəsizliyini daim vacib amil kimi xarakterizə edir. Bu baxımdan smart kart texnalogiyasından əlavə olaraq USBToken və SmartSD kart həllərində ümumi təhlükəsizliyi təmin edən mexanizimlərə çevrilmişdir. Elektron imzanın (e-imza) tətbiqi e-sənəd e-xidmətlərin təhlükəsizliyinin təmin edilməsində vacib yer tutur.**

E–imza yaratma və yoxlama məlumatlarının alqoritmlərinin standartlara uyğunluğu USBToken və SmartSD kart vasitəsi ilə elektron sənədlərin imzalanması və açarların generasiya vaxtı və mexanizmini təmin edilməsi tədqiqat əsasında aparılmalıdır. Məqaləd kriptoqrafik SmartSD kart və Crypto USBToken -lərin köməyi ilə Windows 7 əməliyyat sistemində müxtəlif ölçülü açarların generasiyası və elektron imzanın formalaşmasını təmin edən proqram təminatlarında aparılan ekspermentlərdə əldə edilmiş nəticələrin müqayisəsinə həsr olunmuşdur.

Açar sözlər — PKCS7, e-gov; e-imza; PKİ; e-sənəd; CSP, CA, RSA, SHA-1

I. GİRİŞ

İnformasiya təhlükəsizliyi mühitində məlumat mübadiləsində ötürülən məlumatların səhihliyinin təmin edilməsi və ötürənin identikləşdirilməsi vacib amildir. İnformasiya texnalogiyalarının inkişafı ilə cəmiyyətdə elektron həllərinin təhlükəsizliyinin təmin edilməsi vacibdir. Avropa Birliyinin bu sahədə qəbul etdiyi Direktivə[1] əsasən birliyə daxil olan ölkələr həmin standartlar əsasında işlərə başlamışdılar. Bir çox inkişaf etmiş ölkələrin təcrübəsinə nəzər saldıqda imza sahiblərinin istəklərinə və ya imza təqdim edən mərkəzlərin təklif etdiyi daşıyıcılarda (bura USBToken SmartSD kart daxildir) və s elektron imzaların formalaşmasını təmin edən açarlar və sertifikatlar daxil edilmişdir. Yuxarıda da qeyd edilən kimi e- sənədlərdə imzanın formalaşmasında e-imza daşıyıcıları və onların texniki xarakteristikaları vacib olan təhlükəsizlik meyarlarını özündə ehtiva edir.

II. E-İMZA HƏLLİNDƏ AÇARLARIN SAXLANMA VASİTƏLƏRİ

İmza yaratma (gizli açar) və imza yoxlama məlumatları (açıq açar) müxtəlif növ yaddaş vasitələrində saxlana bilər. Əsas şərt açarların saxlanması üçün seçilən həllin gizli açarın təhlükəsizliyini təmin edə bilməsi və CSP (Kriptoqrafiya Xidməti Provayderi) müxtəlif əməliyyat sistemləri üçün açarlardan və sertifikatdan istifadəni təmin edə bilməsidir. Aşağıdakı CSP-lərə əsasən açarların ölçülərinə görə generasiya vaxtı və MSOffice və P7Signer[2] –imzalayıcının imkanlarından istifadə edərək imzalanma müddətləri ölçülmüşdür.

1) Provider Name: Athena ASECard Crypto CSP
   Provider Type: 1 - PROV_RSA_FULL
2) Provider Name: Gemalto Classic Card CSP
   Provider Type: 1 - PROV_RSA_FULL
3) Provider Name: EnterSafe ET199SD CSP v1.0
   Provider Type: 1 - PROV_RSA_FULL
4) Provider Name: eToken Base Cryptographic Provider
   Provider Type: 1 - PROV_RSA_FULL
5) Provider Name: Oberthur Card Systems Cryptographic
   Provider Type: 12 - PROV_RSA_SCHANNEL
   Provider Name: Charismathics Smart Security Interface
6) *Provider Type 24 - PROV_RSA_AES*

Açarlar proqram təminatı və ya aparat təhlükəsizlik modullarının imkanları vasitəsilə qorunur. Proqram təminatı vasitəsi ilə təmin edilən açarların təhlükəsizliyik səviyyəsi coxd yüksək olmur və nəticə etibarı ilə tam təhlükəsiz sayılmır.

Gizli açarların qorunması üçün aşağıdakı vasitələr istifadə edilir:

- HSM (Hardware Security Module)
- Smart kart
- USBToken
- SmartSD kart

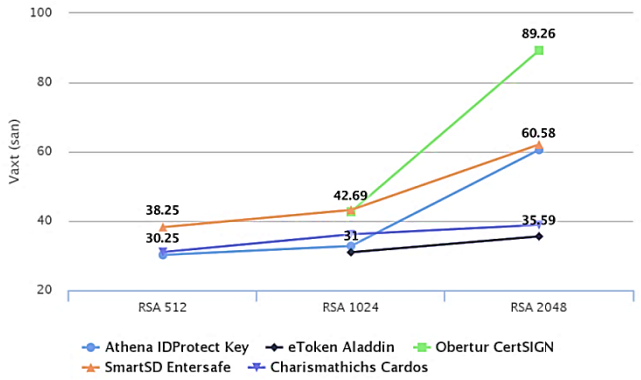
Aşağıdakı cədvəldə kriptopravayderlərə əsaslanaraq müxtəlif ölçülü açarların generasiya müddətləri təqdim edilir.

Cədvəl 1. Sertifikat sorğusunun və açarların generasiyası müddəti

№	Açarların saxlanma sistemlərində generasiya müddəti			
	Gizli açarların qorunma vasitələri	**RSA 512**	**RSA 1024**	**RSA 2048**
1	Athena İDProtect Key	30.25 san	32.81 san	60.58 san
2	eToken Aladdin	**Null**	31 san	35.59 san
3	Obertur CertSİGN	**Null**	42.69 san	89.26 san
4	SmartSD Entersafe	38.25 san	43.22 san	62.11 san
5	Charismathichs Cardos	31.06 san	36.18 san	38.90 san

Null: *–gizli açar qoruyucuları üçün parametrlər təyin edilməyib.*

Aşağıda qeyd olunan Şəkil 1-də Kriptoprovayderlərə əsasən RSA 512, 1024, 2048 bit ölçülü açarlarla sertifikat sorğusu yaranmasının qrafik təsviri öz əksini tapır.



Şəkil 1. Sertifikat sorğusunun yaranması müddəti

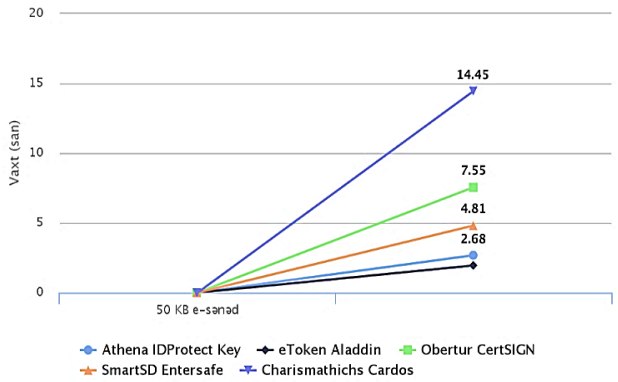
Sertifikat sorğusunun və açarların generasiyasının zamandan asıllığı təsvir edilib.

SmartSD[3] və USBToken açar daçıyıcıları həmçinin konteynerləri şifrələmə funksiyalarına malik xarakteristikalarla təmin edilir.

Növbəti ekspermentdə yuxarıda qeyd olunan CSP-lərə əsaslanaraq RSA 2048 bit SHA1 -ə əsaslanaraq MSOffice və E-imzalayıcının imkanlarından istifadə etməklə ölçmələrin nəticəsi qeyd edilir:

Cədvəl 2. MS Office –də e-sənədin imzalanması müddəti

	e-sənədin MSOffice-də imzalanması (e-sənədin ölçüsü 50 bayt)	
	Gizli açarların qorunma vasitələri	**RSA2048 SHA1**
1	Athena İDProtect Key	2.68 san
2	eToken Aladdin	1.95 san
3	Obertur CertSİGN	7.55 san
4	SmartSD Entersafe	4.81 san
5	Charismathichs Cardos	14.45 san



Şəkil 2. MS Office-də e-sənədin imzalanması müddəti

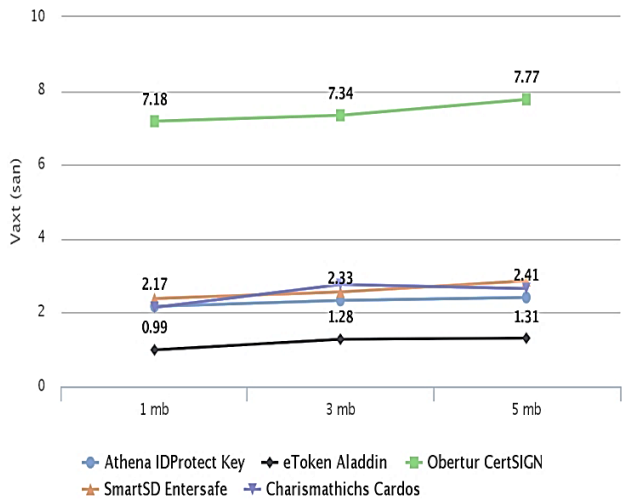
MS Office-də e-sənədin imzalanmasının zamandan asıllığı təsvir edilib.

E-sənədin digər e- imzalayıcı ilə əldə edilməsi zamanı aşağdakı qiymətləndirmələr əldə edilmişdir.

Cədvəl 3. E-imzalayıcıda müxtəlif ölçülü e-sənədlərinin imzalanması müddəti

№	**E-sənədin e-imzalayıcıda imzalanması (e-sənədin ölçüsü 1,3,5 Mb)**			
	Gizli açarların qorunma vasitələri	**1 Mb**	**3 Mb**	**5 Mb**
1	Athena İDProtect Key	2.17 san	2.631 san	2.41 san
2	eToken Aladdin	0.99san	1.28 san	1.31 san
3	Obertur CertSİGN	7.18 san	7.34 san	7.77 san
4	SmartSD Entersafe	2.38 san	2.56 san	2.86 san
5	Charismathichs Cardos	2.14 san	2.76 san	2.65 san

Ekspermentdə yuxarıda qeyd olunan CSP-lərə əsaslanaraq RSA 2048 bit SHA1 -ə əsaslanaraq və E-imzalayıcının imkanlarından istifadə etməklə ölçmələrin nəticəsini zamandan asılılığı müəyyən edilib.



Şəkil 3. PKCS7-də e-sənədin imzalanması müddəti

Müxtəlif tip CSP daşıyıcılarının PKCS7[4] imzalanma həllərinin zamana görə imzalama qrafiki təsvir edilib. Aparılan ölçmələr nəticəsində alınan qrafiklər və cədvəllərdəki qiymətləndirmər belə bir halı özündə əks etdirir ki, CSP –lər[5] özlərinin daxili qurluşu və iş pirinsipi və həmçinin sənəd imzalama sistemləri eyni olçülü məlumatları müxtəlif zaman kəsiklərində icra edirlər. Bu baxımdan e-gov həllərinə və yaxud istənilən informasiya sisteminə e-imza həllərini inteqrasiya etdikdə daşıyıcılar və avadalıqların texniki xarakteristikası işin təşkilinə hər zaman təsir imkanlarına malik ola bilər. CSP-lərə[6] nəzərən alınan nəticələrdən sürətli iş imkanlarına malik olanları müəyyən edib, yüksək sürətlə məlumatların imzalanması və şifrələnməsini təmin etmək mümkündür.

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] Eastlake, D, Reagle, J, Solo, D: XML Signature Syntax and Processing (Second Edition), W3C Recommendation, http://www.w3.org/TR/xmldsig-core

[3] https://www.sdcard.org/developers/overview/ASSD/smartsd/

[4] https://en.wikipedia.org/wiki/PKCS

[5] http://pki.escb.eu/epkweb/pdf/ESCB-PKI-Basic_operations_leaflet.pdf

[6] https://www.charismathics.com/fileadmin/files/pdf/manuals/CSSI_49_EN.pdf