E-imza İnfrastrukturunun Sintezi Problemləri

Həbib Abbasov
AMEA İnformasiya Texnologiyaları İnistutu, NRYTN, Bakı, Azərbaycan
hebib.atilla@gmail.com

***Xülasə*— Müasir dövrdə informasiya texnologiyalarının inkişafı ölkələrin iqtisadi fəaliyyətində onların beynəlxalq və daxili münasibətlərində bütün istiqamətlərdə real çəkiyə malikdir. E-dövlət quruculuğunda, elektron xidmətlərin təşkilində təhlükəsizlik meyyarlarının vacib olması və onun aktual məsələlərdə praktiki tətbiqi e-xidmətlərin dayanıqlılığını və ondan istifadəni vacib edir. Elektron imzanın tətbiqi e-sənəd, elektron bankçılıq, qorunan e-poçt, portal və bulud üzərində e-xidmətlərin təhlükəsizliyinin təmin edilməsində mühüm yer tutur. E-imza infrastrukturuna istifadəçilər tərəfindən olunan müraciətlər və onlara cavablandırılması mexanizmi avtomatik rejimdə icra olunur. Məqalə e-imza infrastrukturunun praktik istifadəsində yaranan texnoloji və problemlərinə həsr olunmuşdur.**

Açar sözlər*— *e-imza, e-dövlət, e-sənəd, açıq açarlar infrastrukturu

I. E-İMZA İNFRASTRUKTURU ÜÇÜN VACİB TƏLƏBLƏR

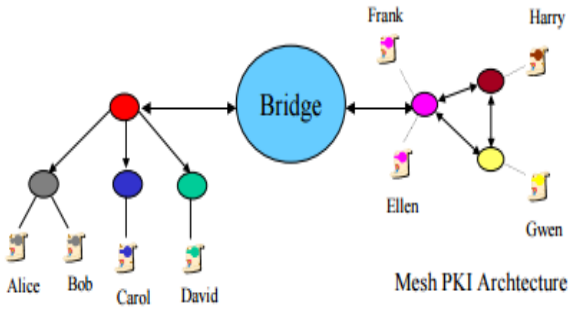
İnformasiya sistemlərinin qarşılıqlı məlumat mübadiləsində ötürülən məlumatların doğruluğu və məlumatın ötürmə mənbəyinin identifikasiya edilməsində e-imza sistemləri informasiya təhlükəsizliyinin əsas vasitələrindən biridir. İnformasiya cəmiyyətinin sürətlə formalaşdığı bir mühitdə e-dövlət həllərinin təhlükəsizliyinin təşkili vacib olan amillərdən biridir. E-dövlət infrastrukturları bir-birindən texniki və texnoloji baxımdan fərqli formada fəaliyyət göstərirlər. Bu tip infrastrukturlarda açıq açarlar infrastrukturu (Public Key Infrastructure, PKI) təhlükəsizliyin əsas komponenti kimi vacib funksiyaları yerinə yetirir. E-imza infrasturukturu formalaşması aşağıda qeyd olunan tələblər əsasında həyata keçirilir [1, 2].

1. Simmetrik şifrləmə alqoritmləri;
2. Rəqəmsal imza alqoritmləri;
3. Kriptoqrafik heş funksiyalar;
4. Açar mübadiləsi alqoritmləri;
5. Simmetrik tamlıq üsulları;
6. Psevdo-təsadüfi ədəd generatorları;
7. Sertifikatlar və ləğv edilmiş sertifikat siyahıları;
8. Fayl zərfi formatları;
9. Repozitarilər;
10. Gizli açar daşıyıcıları;
11. Sertifikatların idarə edilməsi;
12. Tətbiqi proqram interfeysləri (*Application Programming Interfaces, APIs*).

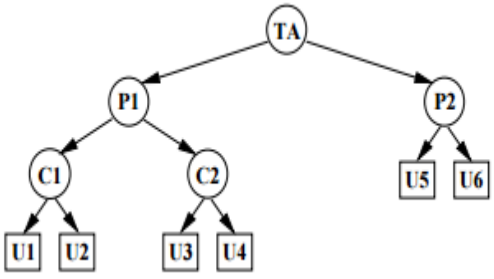
II. E-İMZA İNFRASTRUKTURU MODELLƏRİ

E-imza infrastrukturu üçün bir çox modellər mövcuddur. Aşağıda göstərilən körpü (şəkil 1.) və iyerarxik (şəkil 2.) PKI modelləri geniş istifadə olunur [3].

Sertifikat xidmətləri mərkəzləri bu modellər əsasında bir-biri ilə qarşılıqlı tanınma proseslərini icra edirlər [3]. Hər bir e-imza infrastrukturu öz fəaliyyətini sertifikat siyasəti əsasında təmin edir. E-imza infrastrukturuna daxil olan komponentlər e-dövlət həllərində istifadə edilən identifikasiya sistemidir.



Şəkil 1. Körpü modeli



Şəkil 2. İyerarxik model

Ümumi araşdırmalarda məlum olur ki, hər hansı bir e-imza infrastrukturunun e-dövlət həllərində praktiki tətbiqi zamanı bir sıra problemlər meydana çıxır [4]. Problemləri aşağıdaki kimi qruplaşdırmaq olar.

- ***İnfrastrukturda kriptoqrafik həllər.*** E-imza infrasturkturu qurulan zaman kriptorqafik həllərin qoyulan tələblərlə qurulması məqsədə-uyğundur. Növbəti mərhələrdə RSA həllindən ECC həllinə keçidi təşkil etmək, sistem daxili əlaqələri təmin etmək üçün yeni heş-funksiyalarin tətbiqi nəzərə alınmalıdır.

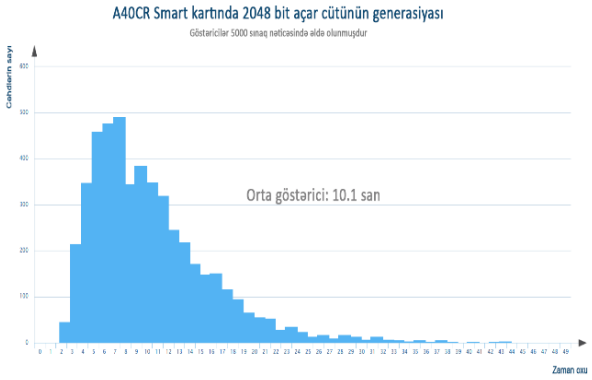
DOI: 10.25045/NCSoftEng.2017.88

- ***Texniki təminatda resursların bölünməsi.*** İnfrastrukturun təşkilində e-imza xidmətləri göstərilən zaman vacib olan xidmətlərin tələb və təklifə əsasən yüksək prioritetə malik olması vacibdir. Vaxt nişanı (*Time Stamp*) və sertifikatlarin online yoxlanılması (OCSP və LDAP) xidmətləri e-imza infrsatrukturunda və e-hökümət sistemlərində icra edilən imza əməliyyatlarında istifadəçilərin autentifikasiyasını və aktiv statusda olduğunu təmin edirlər.

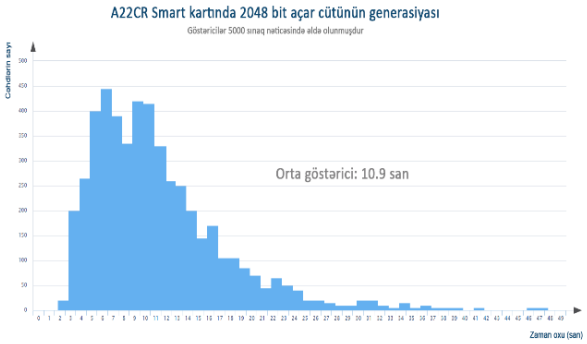
- ***E-imza infrasturkturuna daxil olan açarların və sertifikatların yaradılması üçün daşıyıcıların təşkili.*** Şəkil 3-də A22CR və A40CR Java Card daşıyıcılarının texniki xarakteristikaları göstərilmişdir. Şəkil 4 və şəkil 5-də onlar üzərində müvafiq uzunluqlu açarlar cütünün generasiya üzrə aparılmış testlərin nəticələri, şəkil 6-da isə imza üçün sərf olunan vaxt göstəriciləri təqdim olunmuşdur.

	FT/ A22CR	FT/ A40CR
CPU	16 bit	16 bit
NVM Tipi	Flash (SOLID FLASH)	Flash (SOLID FLASH)
NVM Həcmi	400 kb	240 kb
RAM həcmi	8 kb	6 kb
Transaksiya həcmi	512 bayt	384 bayt
Java Card 2.2.2	+	+
GlobalPlatform 2.1.1	+	+
Çip sertifikatları	CC EAL6+, EMVCo	CC EAL5+, EMVCo

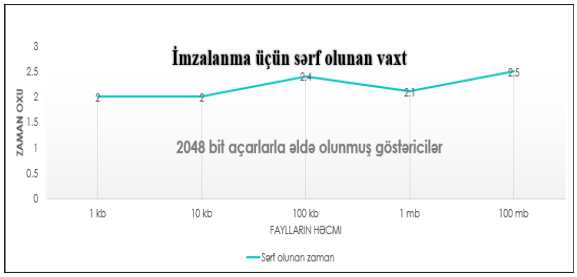
Şəkil 3. A22CR və A40CR Java Card daşıyıcılarının texniki xarakteristikaları



Şəkil 4.



Şəkil 5.



Şəkil 6.

ƏDƏBİYYAT

[1] W3C Recommendation: XML signature syntax and processing (Second edition). 2008. http://www.w3.org/TR/xmldsig-core/.

[2] O. Signore, F. Chesi, M. Pallotti, “E-government: challenges and opportunities,” Proc. of the CMG Italy XIX Annual Conference, pp. 1-16, 2005.

[3] M. Henderson, R. Coulter, E. Dawson, E.Okamoto, “Modelling trust structures for public key infrastructures,” Information Security and Privacy, pp. 203-221, 2002.

[4] C. Adams, S. Lloyd, “Understanding PKI: concepts, standards, and deployment considerations.” Addison-Wesley Professional, 2003

DOI: 10.25045/NCSoftEng.2017.88