Milli e-imza infrastrukturunun təkmilləşdirilməsi problemləri

Həbib Abbasov[1,2]
[1]AMEA İnformasiyaTexnologiyaları İnistutu, Bakı, Azərbaycan
[2] NRYTN Milli Sertifikat Xidmətləri Mərkəzi, Bakı, Azərbaycan
hebib@pki.az

***Xülasə*— İnformasiya cəmiyyətinin üzvləri qlobal şəbəkədə təhlükəsiz formada münasibətlərin tənzimlənməsi üçün müxtəlif autentifikasiya və təsdiqlənmə mexanizimlərindən istifadə edirlər. Bu yanaşmalardan ən geniş istifadə olunanı elektron imza həlləridir. Elektron imza həlləri e-dövlət quruculuğunda hər bir vətəndaş üçün eİD –də (yeni nəsil şəxsiyyət vəsiqəsi) təqdim olunur. Məqalədə bu yanaşmaların daha geniş formada istifadəsini təmin etmək məqsədi ilə məsafədən imzanın verilməsi hüquqi və texnoloji olaraq problemlərin analiz edilməsini eyni zamanda qabaqcıl ölkələrin əldə etdikləri təcrübələri araşdırmaqla milli e-imza infrastrukturunda elmi-praktiki problemləri araşdırılmasına həsr olunmuşdur.**

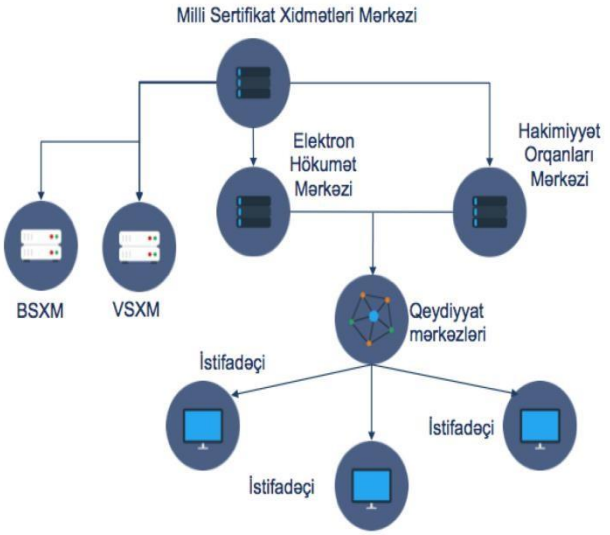
Açar sözlər— e-dövlət; e-imza; e-sənəd; mobil imza; PKI; heş funksiya; sertifikat xidmətləri mərkəzi; eID

I. GİRİŞ

Azərbaycan Respublikasında elektron imza xidmətlərinin həyata keçirilməsi üçün ilk öncə hüquqi baza formalaşmağa başladı və bu istiqamətdə “Elektron imza və elektron sənəd haqqında Qanun” [1] və qanunundan irəli gələn qaydalar təsdiq olundu. Müvafiq qanunun tələblərinə uyğun milli e-imza infrastrukturunun modeli müəyyənləşdi və müvafiq Milli Sertifikat Xidmətləri Mərkəzi (MSXM) yaradıldı. Yaradılan infrastrukturun modeli iyerarxik modelə əsaslanır. Hazırda Əsas (ing. Root) və istifadəçilərə sertifikat verən Elektron Hökumət və Hakimiyyət Orqanları mərkəzləri fəaliyyət göstərir. Fəaliyyəti ilə mərkəzlərin hər biri e-dövlət həllərində tətbiq edilən interaktiv xidmətlərin təhlükəsizliyi üçün istifadəçilərə e-imza və autentifikasiya sertifikatları təqdim edir. Bütün formalaşan sertifikatlar və açarlar beynəlxalq standartlara əsasən formalaşdırılır [2].

II. E-İMZA: HÜQUQİ BAZA VƏ STRUKTUR MODEL

“Elektron imza və elektron sənəd haqqında” Azərbaycan Respublikası qanunu 2004 cü ildə qəbul olundu və Prezidentin 65 nömrəli fərmanı ilə təsdiq olundu. Qəbul edilmiş qanuna əsasən Nazirlər Kabineti müvafiq qaydaları 2006-cı ildə təsdiq edib. Bu hüquqi baza üzərində ölkədə açıq açar infrasturukturu və ondan istifadə mexinizimləri müəyyən edilmişdir. 2011-ci ildə MSXM fəaliyyətə başlamışdır. Mərkəz öz texniki iş funkisyalarını yuxarıda qeyd edilən modelə əsasən təmin edir. Hazırda milli e-imza infrastrukturunda xidmət göstərən sertifikat xidmətləri mərkəzlərinin iyerarxik strukturu şəkil 1-də göstərilib.



Şəkil 1. Milli e-imza infrastrukturunda xidmət göstərən sertifikat mərkəzlərinin iyerarxik strukturu

III. E-İMZA: TƏHLÜKƏSİZLİK ELEMENTİ

Milli e-imza infrastrukturu sistem olaraq təhlükəsizlik komponenti kimi fəaliyyət göstərir. Bu istiqamətdə istifadəçilərə bir çox platforma və üsullarla e-imza sertifikatları təqdim edilir. Bunlar aşağıdakılardır [3]:

- klient əsaslı həllər;
- server əsaslı həllər;
- “online” brauzer əsaslı həllər;
- mobil əsaslı həllər.

Qeyd olunan həllər üzrə proqram təminatı milli e-imza infrastrukturunda təmin edilib. Bu həllər üzrə vacib olan amil kriptoqrafik funksiyaların milli həllərlə icra edilməsini təmin etməkdir.

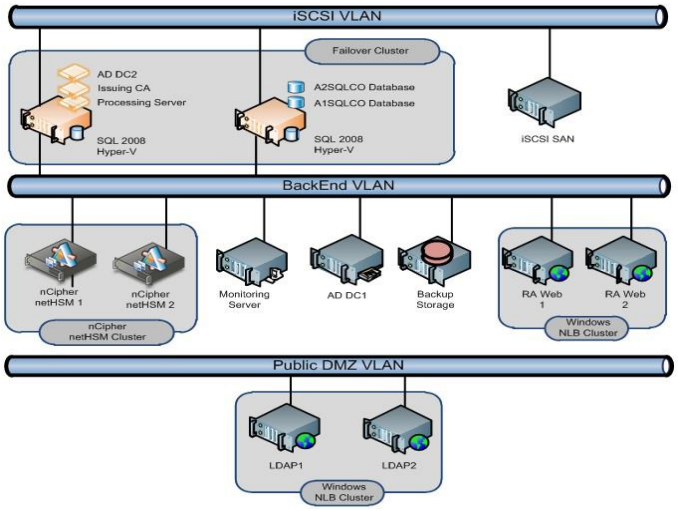
MSXM təqdim etdiyi sertifikatları USBToken və smartkartlar üzərindən icra edir [4]. Qeyd olunan daşıyıcılar xarici vendorlara məxsus olması ilə yanaşı onların əsas CSP (Cryptographic Service Provider, CSP) və RNG (Random Number Generator)[5] kriptoqrafik funkisyaları da özlərinə məxsusudur. Bu sahədə Turkiyə [6] təcrübəsi geniş araşdırma

DOI: 10.25045/NCInfoSec.2017.29

mövzusu oldu və aşağıdakı nəticələr formalaşdı. Türkiyə təcrübəsi göstərir ki, məxsusi olaraq milli CSP [7] və RNG yaradılması və onun üzərində xidmətlərin təşkili təhlükəsiz sistemin formalaşmasına zəmin yaradır. Bu sistemləri (Ağıllı Kart İşlətim Sistemləri) AKİS adlandırırlar. Bu sahədə ölkəmizdə milli həllərin formalaşması vacibdir ki, xarici alqoritimlərdən istifadə və əlavə maddi xərclərdən asılı qalmayaq.

IV. MİLLİ İNFRASTRUKTUR VƏ BULUD ÜZƏRİNDƏ E-İMZA

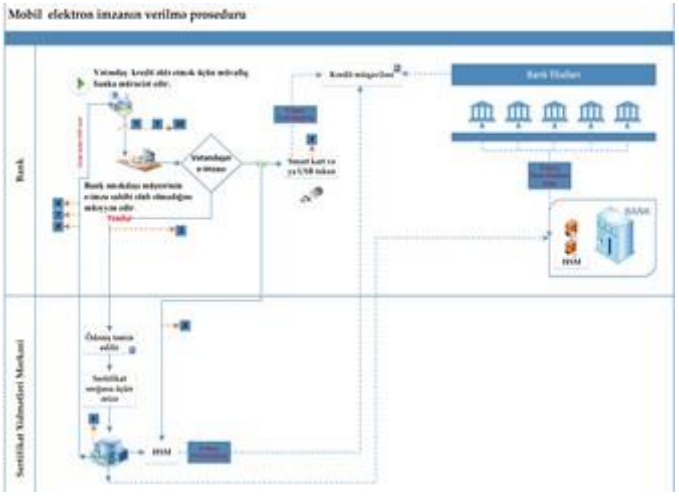
E-imza həlləri üzrə, yuxarıda qeyd olunduğu kimi, geniş formada istifadə sahəsinə malik müxtəlif həllər mövcuddur. Milli e-imza infrastrukturunun ümumi kompüter, server və şəbəkə resurslarınının iş prinsipləri aşağıdakı sxemdə təsvir edilib (şəkil 2).



Şəkil 2. Milli e-imza infrastrukturunun sxematik təsviri

Qeyd olunan sistemi bulud həllərinə uyğunlaşdıraraq mobil imza xidmətləri mexanizmi təşkil edilə bilər. Bu baxımdan müvafiq proqram təminatını və infrastruktura daxil olan platformaları servis vasitəsi ilə təqdim etmək olar. Bu halda gizli açarların qorunması üçün HSM (Hardware Security Module) istifadə edilir. HSM vasitəsi ilə imza xidmətlərinin təklif edilməsi interfeysləri mövcuddur. Nümunə olaraq autentifikasiya Cloud HSM, Avstriya imza sistemi, Cryptomathic və DocuSign və s. xidmət verən platformaları qeyd etmək olar. Hal-hazırda bir çox ölkə: Türkiyə, Norveç, Avstriya və Estoniya bu tip sistemləri özlərində formalaşdırmağa başlamışlar. Qeyd etmək lazımdır ki, Azərbaycanda fəaliyyət göstərən kommersiya fəaliyyətli, Vergilər Nazirliyinə məxsus sertifikat xidmətləri mərkəzi “ASAN imza” adı ilə istifadəçilərə xidmət təqdim edir. Platforma ümumilikdə Estoniya təcrübəsinə əsaslanaraq qurulub və SİM karta əsaslanan imza sertifikatları təqdim edir.

Mobil və elektron imzaların məsafədən alınması və imzalanma prosedurlarının icra edilməsi məqsədi ilə milli e-imza infrastrukturna müəyyən texniki əlavələr edilməklə aşağıdakı struktur sxem tərtib edilmişdir (şəkil 3). Qeyd olunan platforma əsasında hazırlanan imzalar nümunə olaraq ixtiyari korparativ sistemlər və yaxud banklarda tətbiq oluna bilər.



Şəkil 3. Milli e-imza infrastrukturunun bulud üzərində texniki təsvir

NƏTİCƏ

Milli e-imza infrastrukturunda HSM üzərindən mobil qurğuların iştirakı ilə yeni fərdiləşmə mexanizmi yaradılmış və sənədlərin PDF, XML [8] və XADES formatlarında imzalanması mexanizmi tətbiq edilmişdir. Bu sahədə mövcud qanunvericilikdə müvafiq texniki tənzimləmələrin formalaşması vacibdir. Qeyd etmək lazımdır ki, qurulan sistemlər ümumilikdə yerli qanunvericiliyə uyğunlaşdırılır. Bu baxımdan, yüksək qiymətli xarici sistemlərdən asılı olmamaq üçün, mövcud informasiya təhlükəsizliyi siyasəti çərçivəsində milli həllərin formalaşdırılması vacibdir və dövrün tələbidir.

ƏDƏBİYYAT

[1] Elektron imza və elektron sənəd haqqında Azərbaycan Respublikasının Qanunu. 2004-cü il.

[2] 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.

[3] Y.İmamverdiyev, “E-dövlət üçün bulud texnologiyaları əsasında mobil elektron imza,” İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransının əsərləri, s.138-141, 2015.

[4] http://e-imza.az/stats.php?lang =az

[5] https://en.wikipedia.org/wiki/Hardware_random_number_generator

[6] http://www.marmara.edu.tr/en/hizmetler/e-bilgi-servisi/mobil-imza-m-imza/

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

[8] Eastlake D., Reagle J., Solo D. et al. “XML Signature Syntax and Processing Version 2.0)”. W3C Recommendation, 2015.

PROBLEMS OF IMPROVING THE NATIONAL E-SIGNATURE INFRASTRUCTURE

Habib Abbasov[1,2]
[1]Institute of Information Technology of ANAS, Baku, Azerbaijan
[2]National Certificate Services Center of The Ministry of TCHT
hebib@pki.az

Abstract – Members of the information society use different authentication mechanisms to regulate secure relationships on the global network. The most widely used approaches are electronic signature solutions. E-signature solutions are provided in e-ID (new generation ID) for each citizen in e-government. The paper is devoted to the analysis of legal and technological problems and the study of scientific-practical problems in the national e-signature infrastructure by examining the experiences of advanced countries.
Key words – e-government; e-signature; e-document; mobile signature; PKI; hash function; certification service center; e-ID