Etibarlı elektron sənəd dövriyyəsi sistemlərində elektron imza formatları

Ülkər Əliyeva
Azərbaycan Respublikasının Prezidenti yanında Dövlət İdarəçilik Akademiyası
ulker.aliyeva577@gmail.com

***Xülasə*— Məqalədə etibarlı elektron sənəd dövriyyəsi sistemləri üçün nəzərdə tutulmuş elektron imza formatları haqqında ümumi məlumat verilir. Asan imza, gücləndirilmiş elektron imza və təkmil elektron imza nəzərdən keçirilir və CAdES, PAdES və XAdES kimi elektron imza formatları analiz edilir.**

Açar sözlər*— *elektron imza, təkmil imza; gücləndirilmiş elektron imza; elektron imza formatı.

I. GİRİŞ

Kompüter texnologiyalarının inkişaf etməkdə olduğu dünyada informasiya təhlükəsizliyi məsələsi getdikcə daha vacib məsələ kimi ortaya çıxmışdır. Məlumat mübadiləsi zamanı ötürülən informasiyanın təhlükəsizliyinin qorunması çox mühüm məsələdir. Dövlət orqanları ilə müxtəlif əməliyyatlar həyata keçirərkən vətəndaşların şəxsi məlumatlarının üçüncü tərəfin ələ keçirməməsi üçün təhlükəsiz şəbəkələr getdikcə daha çox yayılır. Bundan başqa elektron əməliyyatların həyata keçirilməsi zamanı vətəndaşın kimliyinin ayırd edilə bilməsi də təhlükəsizlik qədər vacib məsələdir. Bütün qeyd olunanlar isə elektron imzanın zəruriliyini ortaya çıxarır. E-imza ilk dəfə Uildfild Diffi və Martin Xellman tərəfindən 1976-cı ildə təklif edilmişdir. 1977-ci ildə ilk kriptoqrafiya alqoritmi RSA yaradılmışdır. Elektron imzanın əsas mahiyyəti informasiyanı hazırlayan şəxsin həqiqiliyinin yoxlanılması və 3-cü tərəfə (məhkəmə, internet market və s.) bu informasiyanı yaradan şəxsi müəyyən etməsinə imkan yaratmaqdır. Hal-hazırda elektron imzanı tətbiq edən ölkələr digərlərinə nisbətən daha inkişaf etmiş hesab olunur və həmçinin belə ölkələrdə inkişaf daha da dinamik baş verir.

Elektron formada təqdim edilən və elektron imza ilə kodlaşdırılan elektron sənədlərin informasiya sistemində nizamlanmış hərəkəti ilə bağlı informasiya proseslərini nəzərdə tutan elektron sənəd dövriyyəsinin tətbiqi zamanı hər kəs yalnız öz səlahiyyətləri daxilində olan məlumatları əldə edə bilir.Bu isə informasiya təhlükəsizliyinin yüksək səviyyədə təminatı deməkdir.

II. ETİBARLI ELEKTRON SƏNƏD DÖVRİYYƏSİNİN TƏLƏBLƏRİ

Elektron sənəd dövriyyəsi vasitələrinə qoyulan tələblər aşağıdakılardır:

- Dövlət orqanlarının mülkiyyətində olan və ya istifadə etdikləri informasiya sistemləri vasitəsilə təhlükəsiz elektron sənəd dövriyyəsinin aparılması məqsədilə müvafiq icra hakimiyyəti orqanı tərəfindən müəyyən edilmiş qaydaya əsasən bu sistemlərin ekspertizası həyata keçirilməlidir;
- Tərkibində dövlət sirri təşkil edən məlumatlar olan və digər konfidensial informasiyaların sertifikatlaşdırılmış mühafizə vasitələri elektron sənəd dövriyyəsində müvafiq icra hakimiyyəti orqanı tərəfindən müəyyən olunmuş qaydada istifadə edilir;
- İstifadə edilən elektron imza və elektron sənəd dövriyyəsi vasitələri sertifikatlaşdırma haqqında Azərbaycan Respublikasının qanunvericiliyinə müvafiq qaydada sertifikatlaşdırılır. [1]

III. ELEKTRON İMZA

Elektron imza elektron dünyada şəxsiyyəti müəyyənləşdirmə vasitəsidir. Elektron imza anlayışı ümumi xarakter daşıyır. İnsanların əl imzalarının rəqəmli çeviricilərdən keçirilmiş, barmaq izləri, səs kimi bioloji əlamətlərinin və s. elektron halda kimliklərinin doğrulanmasını təmin edən vasitədir. Elektron imza elektron sistemdə imzanın malik olduğu bütün işləri yerinə yetirən, elektron sertifikat vasitəsilə bir elektron məlumata əlavə edilən və məlumatı göndərəni təyin edən bir ədədi koddur [2].

Elektron imza digər verilənlərə əlavə edilən və ya onlarla məntiqi əlaqəli olan, imza sahibini identikləşdirməyə imkan verən verilənlərdir. Elektron imza sənədin həqiqiliyi, bütövlüyü və dəyişilməzliyini təmin etməyə imkan verir.

Bu gün elektron hökumətin əsas atributlarından sayılan elektron imza Azərbaycanda uğurla tətbiq edilməkdədir. “Elektron imza və elektron sənəd haqqında” Azərbaycan Respublikasının Qanunu qəbul edildikdən sonra “elektron imza”nın reallaşdırılması mərkəzi icra orqanı kimi Rabitə və İnformasiya Texnologiyaları Nazirliyinə tapşırılmışdır.

Azərbaycan Respublikasının Qanunlarına əsasən elektron imza ilə imzalanmış elektron sənədlər əl imzası ilə imzalanmış və möhürlənmiş sənədlərə bərabər tutulur. Bu gün Azərbaycanda 200 mindən artıq e-imza sahibi vardır. Elektron imza ilə imzalanmış sənədlər bir neçə saniyə ərzində lazım olan yerə çatdırıla bilər. Elektron sənəd mübadiləsinin bütün iştirakçıları bir-birindən uzaqda olmalarına baxmayaraq eyni imkanlar əldə edirlər. Elektron imzanın istifadəsi zamanı elektron sənədlər adi kağız sənədlər kimi hüquqi qüvvəyə malik olur.

Respublikamızda elektron imza sisteminin tətbiqi və dövlət orqanlarında elektron xidmətlərin göstərilməsi gələcəkdə ölkəmizin dünya informasiya sisteminə, Avropaya inteqrasiyasını daha da sürətləndirmiş olacaq.

A. Asan imza(Mobile İD)

Asan İmza (Mobil imza) - Vergilər Nazirliyi və Mobil operator tərəfindən verilən və elektron xidmət istifadəçisinin autentifikasiyasını, sənədin elektron imzalanmasını və imzalayan şəxsin şəxsiyyətinin müəyyən edilməsini (identifikasiyasını) təmin edən xidmətdir.

Asan İmza (Mobil ID) bütün mövcud e-xidmətlərdən istifadəni mümkün edir.Asan İmza (Mobil ID elektron mühitdə fiziki İD-karta bərabər sənəd kimi sertifikatlara bağlı olan mobil telefon SİM-kartıdır.Asan İmza (Mobil ID) ilə şəxsiyyəti təsdiq etmək və sənədlərə rəqəmsal imza atmaq olur. [3]

B. Gücləndirilmiş elektron imza (advanced digital signature)

Gücləndirilmiş elektron imza-imza sahibinin nəzarəti altında olan elektron imza vasitələri ilə yaradılan və yalnız imza sahibinə məxsus olmaqla onu identikləşdirən, əlaqəli olduğu məlumat bildirişinin bütövlüyünü, dəyişməzliyini, təhrif olunmadığını və saxtalaşdırılmadığını müəyyən etməyə imkan verən elektron imzadır.

Gücləndirilmiş e-imzanın üstünlükləri:

- Gizlilik (confidentiality);
- Bütünlük (integrity);
- Tanınma (authentication);
- Məsuliyyətdən yayınmanın mümkünsüzlüyü (non-repudiation). [4]

C. Təkmil elektron imzalar (qualified digital signature)

Təkmil elektron imza - təhlükəsiz imza yaratma qurğusu tərəfindən şifrələnmiş rəqəmsal sertifikatlı müasir elektron imzadır

Təkmil imza tətbiq etmək üçün ən son texnologiyalara cavab verən texniki elementlərdən istifadə olunmalıdır.Təkmil elektron imzanın tətbiqi e-sənədin imzalanma vaxtının birqiymətli təyini və imzalama anında açıq açar sertifikatının statusunun birqiymətli təyini ilə əlaqədar problemləri həll etməyə imkan verir. Elektron sənədin bunun üçün lazım olan rekvizitləri e-imzanın özündə olur. Təkmil e-imza özlüyündə ASN.1 (Abstract Syntax Notation One) formatında strukturlaşdırılmış yazıdır. Təkmil e-imzaya aşağıdakı elementlər daxil edilir:

- imzalanan sənəd;
- imzalanan atributlar (sənədin heş-kodu, sertifikat sahələrinin heş-kodları, sənədin növü və s.);
- sənədin imzası;
- əvvəlki 1-3 bəndlərində göstərilmiş verilənlər üçün alınmış zaman nişanı;
- sertifikatlara və OCSP-cavaba istinadlar;
- əvvəlki 1-5 bəndlərində göstərilmiş verilənlər üçün alınmış zaman nişanı;
- istifadəçinin tam sertifikatı və ləğvetmə siyahısı məlumatları.

Beləliklə, təkmil e-imzada həm e-sənəddəki imzanın həqiqiliyini sübut edən bütün məlumatlar (imzanın imzalayan şəxsə məxsusluğu, sənəddə təhriflərin olmaması), həm də imzalama anını təsdiq edən, eləcə də imza yaratma anında açıq açar sertifikatının qüvvədə olmasını təsdiqləyən bütün məlumatlar olur. [5]

Təkmil elektron imza formatı Avropa Telekommunikasiya Standartları İnstitutunun (European Telecommunications Standards Institute, ETSI) CAdES standartına əsaslanır (ETSI TS 101 733). Bu standartın əvvəlki versiyalarından biri RFC 3126 “Electronic Signature Formats for long term electronic signatures” adı ilə, daha yeni versiyası isə RFC 5126 “CMS Advanced Electronic Signatures (CAdES)”.CAdES standartından başqa XAdES (XML Advanced Electronic Signature, XML əsasında təkmil elektron imza) və PAdES (PDF Advanced Electronic Signature, PDF əsasında təkmil elektron imza) standartları da mövcuddur.

Təkmil e-imzalar aşağıdakı yeni servislərin istifadəsini nəzərdə tutur:

- sertifikatın statusunun OCSP protokolu (Online Certificate Status Protocol) ilə onlayn yoxlanması,
- TSP (Time-Stamp Protocol) protokolu üzrə zaman nişanı xidməti.

D. CAdES (CMS Advanced Electronic Signatures, CMS əsasında təkmil elektron imza).

CAdES (CMS Advanced Electronic Signatures,CMS əsasında təkmil elektron imza) səkkiz profil (forma) müəyyən edir. [6] Hər profil özündən əvvəlki profili genişləndirir:

- **CAdES-BES**, təkmil imzalar üçün Avropa Direktivlərinin hüquqi tələblərinə cavab verən baza formasıdır;
- **CAdES-T** (timestamp), zaman nişanı əlavə edir;
- **CAdES-C** (tam), imzalanan sənədə aid verifikasiya məlumatlarına istinadlar (sertifikatlar və ləğvetmə siyahıları) əlavə edir;
- **CAdES-X** (geniş), CAdES-C-nin daxil etdiyi məlumatlara zaman nişanı əlavə edir;
- **CAdES-X-L** (geniş, uzun müddətli),gələcəkdə orijinal mənbələr olmadıqda belə, imzanı yoxlaya bilmək üçün imzalanmış sənədə qüvvədə olan sertifikatları və ləğvetmə siyahılarını əlavə edir;
- **CAdES-A v2** (arxiv, versiya 2), periodik (məsələn, hər il) zaman nişanı əlavə edilməsini nəzərdə tutur. Ən son CAdES standartında bu profil köhnəlmiş hesab olunur.
- **CAdES-LT** (uzun müddətli), "ağac-heşləmə" alqoritminin və "sübut yazılarının" (RFC 4998) istifadəsi əlavə edilir. Ən son CAdES standartında bu profil köhnəlmiş hesab olunur.
- **CAdES-A v3** (arxiv, versiya 3). Demək olar ki, CAdES problemlərinin hamısını həll edir.

E. XAdES (XML Advanced Electronic Signature, XML əsasında təkmil elektron imza)

XAdES (XML Advanced Electronic Signatures) təkmil elektron imzası XML-DSİG genişləndirilməsi üşün nəzərdə tutulmuşdur.XML-DSİG sənədlərin rəqəmsal imzalanması üçün ümumi çərçivə olsa da, XAdES Avropa İttifaqı Direktivinin 1999/93/EC mənasında inkişaf etmiş elektron

imzanın istifadəsi üçün XML-DSİG-in profillərini dəqiqləşdirir. [7]

XAdES təklif olunan mühafizə səviyyəsində altı müxtəlif profil (forma) müəyyən edir:

- **XAdES-BES**, təkmil imzalar üçün Direktiv hüquqi tələbləri qane edən formasıdır
- **XAdES-T** (timestamp) imtinaların qarşısını almaq üçün zaman nişanı əlavə edir.
- **XAdES-C** (tam) İmzalanmış sənədlərə aid yoxlama məlumatlarına istinadlar (sertifikatlar və ləğvetmə siyahıları) əlavə edir (lakin faktiki məlumatları saxlamır).
- **XAdES-X** (geniş) gələcəkdə mümkün kompromisə qarşı qorumaq üçün XAdES-C tərəfindən təqdim edilən istinadlara zaman nişanı əlavə edir.
- **XAdES-X-L** (geniş, uzunmüddətli) gələcəkdə orijinal mənbə mövcud olmasa belə, imzanı yoxlaya bilmək üçün imzalanmış sənədə faktiki sertifikatları və ləğvetmə siyahılarını əlavə edir.

F. PAdES (PDF Advanced Electronic Signature, PDF əsasında təkmil elektron imza)

PAdES PDF faylının məhdudiyyətlər və genişləndirmələri məcmusudur və ISO 32000-1 təkmil elektron imzasına uyğundur. Bu TS 102 778 kimi ETSİ tərəfindən nəşr olunur.

PAdES PDF faylını və İSO 32000-1 rəqəmsal sənədlərinin imzalanması üçün baza təmin edir, Avropa İttifaqı 1999/93/EC Direktivi mənasında təkmil elektron imzanın istifadəsi üçün profili dəqiqləşdirir. PAdES-in bir mühüm cəhəti ondan ibarətdir ki, əsas kriptoqrafik alqoritmlər pozulasa belə, elektron formada imzalanmış sənədlər uzun müddət qüvvədə qalır. PADES təminat verir ki, rəqəmsal imzalanmış sənədlər uzun illər istifadə oluna bilər. PAdES standartı Direktivin tələblərini təmin etmək üçün bir neçə PDF genişləndirmələrini təqdim edir.

PAdES ETSİ-nin ESİ komitəsi tərəfindən hazırlanmış digər iki elektron imza formatları ilə bir-birini tamamlayır və Avropa İttifaqı çərçivəsində geniş tanınır [8].

PAdES-in əhəmiyyətli üstünlüyü ondan ibarətdir ki, o, PDF genişlənməsi olan faylı proqram təminatı vasitəsilə gətirir: Bu, ixtisaslaşdırılmış proqram təminatından inkişaf və ya adaptasiya tələb olunmur.

PAdES ETSİ texniki spesifikasiyası 6 hissədən ibarətdir:

1-ci hissə: PAdES icmal - PAdES üçün çərçivə sənədi.

2-ci hissə: PAdES Əsas - İSO 32000-1 əsasında profil.

3-ci hissə: PAdES Gücləndirilmiş - PAdES-baza elektron imza və PAdES-açıqlama siyasəti, elektron imza profilləri

4-ci hissə: PAdES uzunmüddətli - PAdES-uzunmüddətli dəyərləndirmə profili

5-ci hissə: XML kontenti üçün PAdES - PDF fayllarının XML kontentdə XAdES imzası üçün profillər

6-ci hissə: Elektron imzanın vizual təsvirləri.

ƏDƏBİYYAT

[1] "Elektron imza və elektron sənəd" haqqında Azərbaycan Respublikasının Qanunu

[2] e-imza.az

[3] taxes.gov.az

[4] e-imza.gov.az

[5] R.M.Əliquliyev,Y.N.İmamverdiyev"Rəqəm imzası texnologiyası" Bakı:Elm,2003.

[6] ETSI, "CMS Advanced Electronic Signatures (CAdES), Version 1.8.1," ETSI, ETSI TS 101 733, Dec. 2009.

[7] ETSI, "PDF Advanced Electronic Signature Profiles, Part 1 - 5," ETSI, ETSI TS 102 778, 2009.

[8] ETSI, "Technical Specification XML Advanced Electronic Signatures (XAdES), Version 1.4.1," ETSI, ETSI TS 101 903, Jun. 2009.