15. Lefevr, P'er. Vozmozhnosti arhitektury dlja ustojchivogo goroda. Institut Francais, Paris-Tashkent, 2013
16. Evstaf'ev A. I., Avdeeva T. T. Regulirovanie prostranstvennogo razvitija goroda na osnove devolopmenta lokal'nyh gorodskih territorij. https://cyberleninka.ru/article/v/regulirovanie-prostranstvennogo-razvitiya-goroda-na-osnove-developmenta-lokalnyh-territoriy, 2011
17. Burdett Richard., Kanai Miguel. City- building in an age of global urban transformation. Cities. Architecture and Society. 10 Mostra Internazionale de Architettura, Venecia. 2006

Redaksiyaya daxil olma/Received 19.03.2020
Çapa qəbul olunma/Accepted for publication 21.04.2020

İNŞAAT

СТРОИТЕЛЬСТВО **CONSTRUCTION**

ELEKTRON İMZANIN YARADILMA VƏ İDENTİFİKASİYA SİSTEMİNİN TƏHLİLİ

Babayev Eltəkin Zəfər oğlu- f.r.e.n., dosent, Geomatika kafedrası, AzMİU, eltakinb@risk.az
Miriyeva Nərgiz SeyidƏli qızı– f.r.e.n, dosent, İT və proqramlaşdırma kafedrası,
Azərbaycan Texniki Universiteti, nargiz.miriyeva@yandex.ru

Annotasiya. Elektron imzanın iş prinsipi, elektron imza növləri, elektron imza sxemlərinə hücumların təsnifatı, elektron imza quruluş sxemləri, elektron imzanın formalaşdırılma sxemləri və elektron imza identifikasiya sisteminin təhlili nəzərdən keçirilib. Elektron imzanı alarkən əvvəlcə sertifikat və açar faylları yaratmaq lazımdır. Sertifikat mərkəzləri sertifikatların istifadəsi üçün tənzimləyici, təşkilati və hüquqi əsaslara zəmanət verir. Sertifikata əlavə olaraq hər bir istifadəçinin bir cüt açara ehtiyacı var-gizli və açiq. Açarlar sertifikatlaşdırma orqanlarında yaradıla bilər və sertifikatla birlikdə istifadəçilərə ötürülə bilər. Ancaq burada Sertifikat Mərkəzinin özündə məxfiliyin pozulması və informasiya təhlükəsizliyinə uyğun olma təhlükəsi var.İstifadəçi həmçinin iş yerində açarları yarada və sonrakı sertifikat istehsalı üçün açarın açıq hissəsini sertifikatlaşdırma mərkəzinə verə bilər. Açar açıq kanallar üzərindən ötürülürsə, dəyişdirilə bilər. Sonra mesajın yoxlanılması səhv açarla aparılacaq və düzgün rəqəmsal imza digər iştirakçılar tərəfindən saxta kimi qəbul ediləcək.
Açar sözlər: elektron imza, heş-funksiya, identifikasiya, kriptodavamlığıdır, simmetrik şifrələmə , hücumlar

ANALYSIS OF THE ELECTRONIC SIGNATURE CREATION AND IDENTIFICATION SYSTEM

Babayev Eltəkin Zəfər- PhD of phys. and math. sci., ass. prof., department of Geomatika,
AzUAC, eltakinb@risk.az
Miriyeva Nərgiz SeyidƏli- PhD of phys. and math. sci, ass. prof.,
department of IT and Programming**,** Azerbaijan Technical University**,** nargiz.miriyeva@yandex.ru

Abstract. The principle of electronic signature operation is considered, types of electronic signature, classification of attacks on electronic signature schemes, schemes for building an electronic signature, electronic signature generation schemes, and also an analysis of the electronic signature identification system.When receiving an electronic signature, you must first create a certificate and key files. Certification centers guarantee the regulatory, organizational, and legal basis for the use of certificates. In addition to the certificate, each user needs a pair of keys- secret and open. Keys can be created by certification agencies and passed to users together with the certificate. However, there is a risk of breach of confidentiality and compliance with information security in the Certification Center itself. User can also create keys in the workplace and give the open part of the key to the certification center for further certificate production. If the key is transmitted through open channels, it can be changed. Then, message will be verified with the wrong key, and correct digital signature will be received as false by other participants.
Keywords: electronic signature, hash function, identification, cryptographic security, symmetric encryption, attacks

Hesablama texnikasının və informasiya texnologiyalarının inkişafı, eləcə də kompüter şəbəkələrinin uzun olması ilə əlaqədar kompüter şəbəkələri vasitəsi ilə ötürülən məlumatların icazəsiz girişdən qorunmasına daha çox diqqət yetirilir. Elektron imza (Eİ)- sənədin xüsusi rekvizitidir, hansı ki, Eİ- nin formalaşdığı andan elektron sənəddə informasiyanın təhrif olunmamasını müəyyən etməyə və onun sahibinə mənsubluğunu təsdiqləməyə imkan verir [1].

Təsadüfi və ya qəsdən bir dəyişiklik olduqda, rəqəmsal imza etibarsız olur. Elektron imzanın istifadəsi, ötürülən sənədin hər hansı məlumatlarının təhrif edilməsinin aşkarlanmasına zəmanət verir. Gizli açar yalnız sənədin sahibində ola bilər ki, bu da müəllifliyini birmənalı sübut etməyə imkan verir. Elektron imzaların *üç növü* vardır:

- sadə imza sənədin müəllifini müəyyənləşdirməyə imkan verir, lakin sənəddə dəyişikliklər olmasını yoxlamaga imkan vermir;
- gücləndirilmiş ixtisaslaşmamış imza təkcə müəllifi tanımağa deyil, sənəddəki dəyişiklikləri də qeyd etməyə imkan verir. Möhürü olan bir sənədin analoqu kimi qəbul edilir;
- gücləndirilmiş ixtisaslı imza [2].

Aşağıdakı *əsas anlayışları* qeyd edək:

- elektron imza yoxlama açar sertifikatı- təsdiqedici mərkəz tərəfindən verilən və Eİ yoxlama açarının sertifikat sahibinə mənsubluğunu təsdiq edən sənəd;
- elektron imza açarı (gizli açar)- imza yaratmaq üçün unikal simvol ardıcıllığı. Gizli açarı yalnız sənəd göndərəndə var;
- elektron imza yoxlama açarı (açıq açar)- imzanı yoxlamaq üçün unikal simvol ardıcıllığı. Paylaşılan (açıq) bir resursda yerləşdirilir və ya lazım olan hər kəsə göndərilir. Açıq açar gizli açara əsaslanaraq hesablanır və onun üçün cütləşir.

Elektron imzanı alarkən əvvəlcə sertifikat və açar faylları yaratmaq lazımdır. Onların yaradılması zamanı xüsusi kriptoqrafik proqramlardan– kriptoprovayderlərdən istifadə olunur. Sertifikatlar müvafiq lisenziyaları olan təsdiqedici mərkəzlərdə verilir.

Sertifikat mərkəzləri sertifikatların istifadəsi üçün tənzimləyici, təşkilati və hüquqi əsaslara zəmanət verir. Sertifikata əlavə olaraq hər bir istifadəçinin bir cüt açara ehtiyacı var- gizli və açiq. Açarlar sertifikatlaşdırma orqanlarında yaradıla bilər və sertifikatla birlikdə istifadəçilərə ötürülə bilər. Ancaq burada Sertifikat Mərkəzinin özündə məxfiliyin pozulması və informasiya təhlükəsizliyinə uyğun olma təhlükəsi var.

İstifadəçi həmçinin iş yerində açarları yarada və sonrakı sertifikat istehsalı üçün açarın açıq hissəsini sertifikatlaşdırma mərkəzinə verə bilər. Açar açıq kanallar üzərindən ötürülürsə, dəyişdirilə bilər. Sonra mesajın yoxlanılması səhv açarla aparılacaq və düzgün rəqəmsal imza digər iştirakçılar tərəfindən saxta kimi qəbul ediləcək. Digər vacib məsələ gizli açarın saxlanılmasıdır. Gizli açarın saxlanılmasına görə sahib özü məsuliyyət daşıyır. Həm açar, həm də sertifikat fayllarda saxlanılır. Bu fayllar kompüterin sərt diskində saxlanıla bilər və onları bir parol ilə açа bilər, lakin sonra gizli açarın təhlükəsizliyi bu kompüterin təhlükəsizliyindən asılıdır və baryerlərdən keçməyin bir çox yolu var.

Əsas çatışmazlıq ondan ibarətdir ki, lazımi sənədləri yalnız bu kompüterdə imzalamaq mümkün olacaqdır. Əlavə təhlükəsizlik üçün gizli açari çıxarıla bilən daşıyıcıda saxlanılır (məsələn, PİN ilə ixtisaslaşdırılmış smart kartda). Elektron rəqəmsal imza, rəsmiləşdirilmiş bir quruluş, bir sıra mütləq və məcburi olmayan rekvizit- imza atributlarından ibarət elektron sənəddir. Məcburi atributlara məlumatların etibarlı identifikasiyası və autentifikasiyasını təmin edən kriptoqrafik hissə daxildir.

Elektron rəqəmsal imza yaradarkən əksinə istifadə olunan asimmetrik şifrələmə sxemindən istifadə olunur. Göndərən məlumatı sənədin nəzarət məbləğini hesablayaraq imzalayır, sonra onu gizli açarla şifrələyir və şifrəni mesaja əlavə edir. Açıq açar alıcıda yerləşir. Məlum açara görə qapalı açarı tapmaq mümkün deyil.

Əsas vəzifə göndərənin həqiqiliyini və mesajın bütövlüyünü təmin etməkdir. Şifrələmənin əsasında həlli çətin olan riyazi problem durur. Bunu həll etmək üçün əlavə məlumat lazımdır. Bu əlavə məlumat gizli açardır. Onu bilmədən, şifrələnmə proseduru exponential vaxt aparır. Alıcı açıq açarı imzaya tətbiq edir.

Əgər alınmış nəticə sənədin nəzarət məbləği ilə üst-üstə düşürsə, onda yoxlama yerinə yetirilib, sənəd isə həqiqi sayılır. Çox sayda imzalanmış sənədləri ələ keçirdikdən sonra da təcavüzkar polinom vaxtında lazımi parametrləri hesablaya bilmir. Nəzarət məbləğlərini hesablamaq üçün kriptodayanıqlı haş funksiyasından istifadə oluna bilər. Bu funksiyanın işinin nəticəsi haş, haş kodu və ya Digest adlanır.

Haş funksiyası aşağıdakı xüsusiyyətlərə malik olan dönməz məlumat transformasiyasıdır: transformasiya alqoritminin girişinə ixtiyari uzunluqlu ikili məlumat bloku daxil olur, çıxışda Sabit uzunluqlu ikili məlumat bloku əldə edilir, çıxış dəyərləri mümkün nəticələrin bir sıra boyunca vahid qanunla bölüşdürülür. Alqoritmin girişindəki ən azı 1 bit dəyişəndə onun çıxışı əhəmiyyətli dərəcədə dəyişir. Əgər h haş funksiyasının dəyərini bilsək, M mesajını tapmaq üçün, H(M)= h, hesablama baxımından çətin olmalıdır və verilmiş M mesajı üçün başqa bir M 'mesajı tapmaq problemi H(M)= H(M') hesablama baxımından da çətin olmalıdır.

Yaradılan haş dəyəri mesajları özünəməxsus şəkildə müəyyənləşdirir və ötürülmə zamanı mesajı dəyişdirmək üçün hər hansı bir cəhd qəbul edən tərəfdə heşləmə və ötürücü tərəfdə alınan həzm ilə müqayisə edilərək aşkar ediləcəkdir. Digest üzrə ilkin mesajın alınması mümkün olmadığı üçün bu funksiyalar birtərəfli şifrələmə funksiyaları da adlanır. 160 bitlik eni iki fərqli sənəddə eyni haş məbləğinin olmamasını təmin edir.

Belə bir hadisə haş kolliziyası adlanır, yəni təcavüzkarın eyni haş məbləği olan iki fərqli sənəd əldə etmək cəhdi. Eyni haş məbləği olan sənədlərin nəzəri cəhətdən limitsiz sayı mümkündür. Lakin, "paradoks ad günləri" teoreminə əsasən, N- bit haş məbləği üçün bir toqquşma yaratmaq üçün $2^{\frac{n}{2}}$ sənəd lazımdır. Demək olar ki, bu haş məbləği və sənəd arasında qarşılıqlı birmənalı uyğunluq deməkdir. Elektron rəqəmsal imza sənədin özü deyil, yalnız onun haş məbləği tərəfindən imzalandığından, böyük məlumat blokunun qorunması problemi Sabit uzunluğun daha kiçik məlumat blokunun qorunması probleminə gətirib çıxarır.

Əgər alıcı imzanın həqiqiliyini və sənədin dəyişməzliyini yoxlamalıdırsa, o, ictimai açarın imzasını deşifr etməli və nəticəni əldə edilmiş sənədin haş məbləği ilə müqayisə etməlidir. Dəyərlər uyğun gəlsə, göndərənin həqiqiliyi və mesajın bütövlüyü sübut olunur.

Kriptoqrafik hissəyə əlavə olaraq elektron rəqəmsal imza bəzi texniki məlumatları da özündə cəmləşdirir. Buraya imzalanma tarixi və vaxtı, imzanın yoxlanılması üçün əlavə mexanizmlər üçün məlumatlar, imza barədə minimal məlumat, imzanın qrafik təsviri və digər məlumatlar daxildir.

Elektron rəqəmsal imza qoşulmuş (attached signature) və ayrılmış (detached signature). Qoşulmuş imza halında yeni elektron rəqəmsal imza faylı yaradılır ki, bu da imzalanan Faylın məlumatlarını yerləşdirərək, özünəməxsus zərf əmələ gətirir. Yəni həm məlumat, həm də imza ayrılmaz şəkildə bağlıdır və bu, məlumat ötürülməsini asanlaşdırır. Nöqsanlar, məlumatlarla tanış olmaq üçün onları zərfdən çıxarmaq lazım olduğunu- elektron rəqəmsal imzanı çıxarmaqdır.

Ayrılmış imza halında, imza və imzalanan fayl üçün ayrı-ayrı fayllar yaradılır və dəyişdirilmir. Məlumatlarla sərbəst tanış ola bilərsiniz və yalnız şübhə halında elektron rəqəmsal imzalı bir sənəd istifadə etmək lazımdır. Ancaq saxlamaq və köçürmək üçün birdən çox fayl olacaq və ayrılmış imza imzalanan məlumatlara bağlı olmadığı üçün təhlükəsizlik problemləri artır. "Genişləndirilmiş" və "təkmilləşdirilmiş" elektron rəqəmsal imzalar da məlumdur. Elektron imzanın yoxlanılması üçün xüsusi vasitələr və mexanizmlər üçün nəzərdə tutulan istifadə şərtlərinin yoxlanması üçün əlavə məlumat olan adi elektron imzalardır. Lakin bu əlavə xüsusiyyətlər məcburi deyil və imza standart prosedurlarla təsdiq edilə bilər.

Beləliklə elektron imzanın iş prinsipi: sənəd əsasında kriptoqrafik heş funksiyası hesablanır, nəticədə bir heş əldə edilir- sabit uzunluğlu qısa sətir simvoları. Sonra, sənədin özünün imzasını əldə etmək üçün, ortaya çıxan heş qizlı açardan istifadə edərək şifrələnir. Alıcı açıq açarı tətbiq edərək və əldə edilən sənədin heşin hesablamaqla sənədi şifrələyə bilər. Sənədi alan açiq açardan istifadə edərək və əldə edilən sənədin heşini hesablayaraq sənədi açа bilər.

Sənədin heşi göndərilməzdən əvvəl və alındıqdan sonra üst- üstə düşərsə, onda sənəd əsl sayılacaq. Əks halda, sənədin dəyişdirildiyi və ya saxtalaşdırıldığı düşünülür. Bu elektron imzaya hücum səbəbindən baş verə bilər [3].

Eİ sxemlərinə hücumların aşağıdakı təsnifatı mövcuddur:
– açıq açarı istifadəsi ilə hücum;
– imzalanmış məlumatlara əsaslanan hücum (təcavüzkarın açıq açarla yanaşı, bir sıra imzalanmış məlumatları olduqda);
– imzalanmış məlumat seçimi ilə sadə hücum (təcavüzkar məlumat seçə bilər, məlumat seçdikdən sonra artıq açıq açar əldə edə bilər);
– məlumat seçimi ilə hədəf hücum;
– seçilmiş məlumatlara əsaslanan adaptiv hücum.

Bu cür hücumların nəticəsi həm tam elektron imzanın sındırılması, həm də onun tam (və ya qismən seçilmiş) saxtalığı ola bilər.

Bu baxımdan elektron imza üçün əsas meyar onun kriptodavamlığıdır, yəni müxtəlif növ hücumlara qarşı davamlılıq , hansı ki onun yaranma metodu (alqoritmi) ilə müəyyən edilir.
Eİ- ni kriptodavamlığa təhlil edərkən, ilk növbədə seçilmiş məlumatlar əsasında adaptiv bir hücum nəzərə alınır, çünki o ən təhlükəli hesab olunur [4].

Elektron imza yaratmaq üçün iki sxem mövcuddur:
- simmetrik şifrələmə alqoritmlərinə əsaslanan. Burada, etibarlılığı kifayət qədər yaxşı öyrənilmiş blok şifrələri istifadə olunur. Əgər hansı bir konkret tapşırıq üçün şifrənin davamlığı yetərli deyilsə, onu asanlıqla daha davamlı şifrə ilə əvəz etmək olar. Lakin bu halda ötürülən məlumatların hər bitini imzalamaq lazımdır. Bu isə imzanın ölçülərini artırır. İmza üçün yaradılan açarlar yalnız bir dəfə istifadə edilə bilər;
- asimmetrik şifrələmə alqoritmlərinə əsaslanan. Hal- hazırda bu üsul daha çox istifadə olunur (bu halda sənədin imzalanması üçün cüt açar istifadə olunur).

Asimmetrik şifrələmə alqoritmlərinə əsaslanan elektron imzanın formalaşdırılması üçün bir çox müxtəlif növ sxemlər mövcuddur. Məsələn:
- Əl- Qamal sxemi;
- ABŞ elektron rəqəmsal imza standartları: DSA, ECDSA;
- FDH (FullDomainHash), RSA-PSS (ProbabilisticSignatureScheme) ehtimal sxemi, PKCS#1 standartın sxemi və RSA alqoritminə əsaslanan digər sxemlər;
- elektron rəqəmsal imza üçün Rusiya standartı: QOST R 34.10-2012;
- Diffi- Helman sxemi;
- Şnopp sxemi;
- Pointcheval- Sternsignaturealgorithm;
- BLS (Boneh- Lynn- Shacham) sxemi;
- GMR (Goldwasser- Micali- Rivest) sxemi;
- Rabinin imza üçün ehtimal sxemi. [5].

Hal- hazırda onlardan ən çox istifadə edilən RSA və Əl- Qamal alqoritmləridir.

Yuxarıda göstərildiyi kimi, elektron imza sənədin özünə deyil, heş- ə yerləşdirilir (imzalanan sənədin dəyişən həcmi nəzərə alınır). Bu heşi hesablamaq üçün müxtəlif heş funksiyalardan istifadə olunur. Özü- özlüyündə heş funksiyası elektron imza yaratma alqoritminin bir hissəsi deyil. Buna görə də hər hansı bir etibarlı alqoritm istifadə edilə bilər (məsələn, SHA, MD5 və QOST 34.11-2012) [6].
Ən tanınmış heş- funksiya SHA- dır. Bu funksiya sıxılma ideyası üzərində qurulub. İlkin məlumat hər birində 512 bit olan bloklara bölünür. Sonuncu belə blokda ilkin məlumatın uzunluğu barədə məlumatlar yazılır.
Heş funksiyaların istifadəsində bir sıra üstünlükləri var:
- hesablama mürəkkəbliyi. Heşin imzalaması sənədin özünü imzalamaqdan daha az vaxt tələb edir (həcmi daha kiçik olduğuna görə);
- uyğunluq. İstənilən mətni uyğun bir formata çevirmək üçün heş funksiyadan istifadə edilə bilər, çünki fərqli alqoritmlər məlumatları fərqli formatından istifadə edir;
- bütövlük. Bəzi sxemlər üçün böyük sənədin kiçik bloklara bölünməsi tələb edir. Lakin identifikasiya zamanı (heş funksiyasından istifadə edilmirsə) bütün blokların çatdırıldığını və düzgün qaydada təyin olunduğu müəyyən etmək mümkün deyil.