DOI: https://doi.org/10.36719/2789-6919/19/26-29

Bəxtiyar Kərimov
Azərbaycan Dövlət Neft və Sənaye Universiteti
magistrant
bextiyarkerimov99@mail.ru

RƏQƏMSAL İMZA VƏ SERTİFİKATLAR

Xülasə

İnternetin inkişafı ilə rəqəmsal imza təhlükəsizlik üçün bütövlüyü və məxfiliyinə görə getdikcə daha çox əhəmiyyət kəsb edir. Açıq şəbəkələr üzərində təhlükəsiz əməliyyatlar üçün Rəqəmsal İmza konsepsiyası gərəkli olur. Məqalədə rəqəmsal imzanın nəzəri və texnologiya bazası olan PKI (Public Key Infrasturucture – Açıq Açar İnfrastrukturu) haqqında məlumat verilir. Gizli və Açıq açara əsaslanan rəqəmsal imzaların əsas tətbiq üsulları, rəqəmsal sertifikat əsasında rəqəmsal imza yanaşması təqdim olunur. Onun rasionallığı, effektivliyi və mümkünlüyü müzakirə olunur.

Açar sözlər: *Açıq açar, gizli açar, heş funksiyası, rəqəmsal imza, rəqəmsal sertifikat*

Bakhtiyar Karimov
Azerbaijan State Oil and Industry University
master student
bextiyarkerimov99@mail.ru

Digital signatures and certificates

Abstract

With the development of the Internet, digital signatures are becoming more and more important for security due to their integrity and confidentiality. The concept of Digital Signature is necessary for secure transactions over open networks. The article provides information about PKI (Public Key Infrastructure), which is the theoretical and technological basis of digital signature. The main application methods of digital signatures based on Private and Public key, digital signature approach based on digital certificate are presented. Its rationality, effectiveness and feasibility are discussed.

Keywords: *Public key, private key, hash function, digital signature, digital certificate*

Giriş

Bank işi, birja ticarəti və malların alqı-satqısı kimi tətbiqlər əməliyyat xərclərini minimuma endirmək və təkmilləşdirilmiş xidmətlər təqdim etmək üçün elektron əməliyyatları getdikcə daha çox istifadə edirlər. Bu, kompüterlərdə yaradılan, işlənən və saxlanılan, şəbəkələr üzərindən ötürülən elektron sənədlərin həcmində inanılmaz artımlara səbəb olur. Həmin proqramlarda idarə olunan bu elektron məlumatlar qiymətli və həssasdır, zərərli üçüncü tərəflərin müdaxiləsindən qorunmalıdır. Ənənəvi olaraq, kağız sənədlər orijinallığı təmin etmək üçün kifayət qədər yaxşı işləyən yazılı imzalarla təsdiqlənir. Elektron sənədlər üçün də oxşar mexanizm zəruridir. Rəqəmsal imza alqoritmindən istifadə etməklə yaradılan birlər və sıfırlar sətirindən başqa bir şey olmayan rəqəmsal imzalar, elektron sənədin təsdiqi və autentifikasiyası məqsədinə xidmət edir (1; 2).

Etibarlı rəqəmsal imza alıcıya imkan verir ki, mesajın əvvəlcədən təyin olunmuş şəxs tərəfindən göndərildiyinə və heç bir dəyişikliyə uğramadığına inana bilsin. Rəqəmsal imzalar adətən proqram təminatının paylanması, maliyyə əməliyyatları və başqa, saxtakarlığa rast gəlməyin mümkün ola biləcəyi digər hallarda istifadə olunur. Adi həyat tərzimizdə İnternet ayrılmaz bir hissəyə çevrilib. Təhlükəsizlik bu baxımdan vacib bir termindir. Ciddi hücum baş verərsə rabitə, ticarət əməliyyatları və digər mühüm funksiyalar bu hücumdan təsirlənə bilər (3; 4).

Rəqəmsal imza nədir?

Rəqəmsal imza e-poçt mesajları, makroslar və ya elektron sənədlər kimi rəqəmsal məlumatlar üzərində elektron, şifrələnmiş, identifikasiya möhürüdür. İmza, məlumatın imzalayandan gəldiyini və dəyişdirilmədiyini təsdiqləyir. Rəqəmsal imza imzalayanın şəxsiyyətini yoxlayır və göndərilən sənədlərin saxtalaşdırılmamasını və ya dəyişdirilməməsini təmin edir. Rəqəmsal imza sadəcə sıfırlar və birlər ardıcıllığı olduğundan, onun aşağıdakı xüsusiyyətlərə malik olması arzu edilir:

- Nəticədə imza, imzalanan mesajdan asılı olan bit model olmalıdır (beləliklə, eyni müəllif üçün rəqəmsal imza fərqli sənədlər olacaq);
- İmza həm saxtakarlığın, həm də inkarın qarşısını almaq üçün göndərici üçün unikal olan bəzi məlumatlardan istifadə etməlidir;
- İmzanı yaratmaq nisbətən asan olmalıdır;
- Rəqəmsal imzanın həqiqiliyini tanımaq və yoxlamaq nisbətən asan olmalıdır;

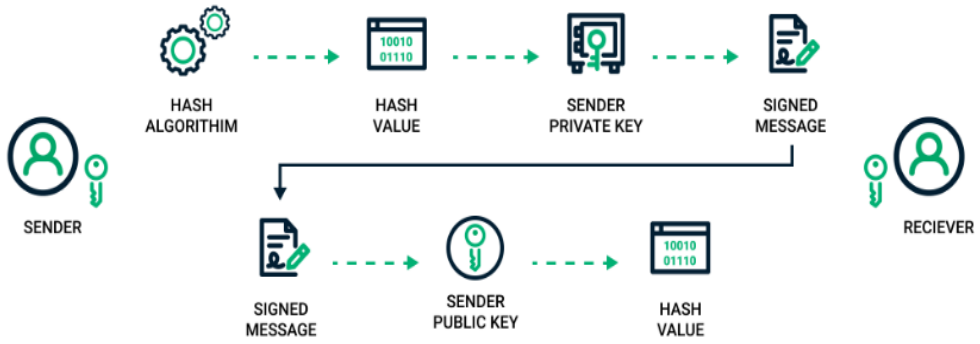
Ya mövcud rəqəmsal imza xarakteri üçün yeni mesaj yaratmaq, ya da verilmiş mesaj üçün saxta rəqəmsal imza qurmaq yolu ilə rəqəmsal imzanın saxtalaşdırılması hesablama baxımından qeyri-mümkün olmalıdır (2; 5; 6).

Rəqəmsal imzalar imzalanmalı olan sənədlərə (mesaj və ya məlumat) və yalnız göndəricidə olan bəzi şəxsi məlumatlara əsasən hesablanır. Praktikada bütün mesajdan istifadə etmək əvəzinə mesajın xülasəsini (digest) əldə etmək üçün mesaja heş (hash) funksiyası tətbiq edilir. Bu kontekstdə heş funksiya giriş kimi ixtiyari ölçülü mesaj alır və çıxış kimi sabit ölçülü mesaj xülasəsini yaradır. Praktikada geniş istifadə olunan heş funksiyalar arasında MD-5 (Message Digest 5) və SHA (Secure Hash Algorithm) var. Bu alqoritmlər kifayət qədər mürəkkəbdir və iki müxtəlif mesajın eyni heş dəyərinə uyğunlaşdırılma ehtimalının çox az olmasını təmin edir. Rəqəmsal imzanın hesablanmasında istifadə olunan iki geniş texnika mövcuddur – simmetrik açar kriptosistem və açıq açar kriptosistem. Simmetrik açar sistemində yalnız göndəriciyə və qanuni qəbulediciyə məlum olan gizli açardan istifadə olunur. Bununla belə, hər iki istifadəçi cütü arasında unikal açar olmalıdır. Beləliklə, istifadəçi cütlərinin sayı artdıqca, gizli açarları yaratmaq, yaymaq və izləmək olduqca çətinləşir (7; 8).

Açıq açar kriptosistemi isə bir cüt açardan istifadə edir: yalnız sahibinə məlum olan gizli açar və sahibi ilə ünsiyyət qurmaq istəyən hər kəsə məlum olan açıq açar. Göndəriləcək mesajın məxfiliyi üçün o, sahibinin gizli açarı ilə şifrələnir. Mesaj yalız mesajı alacaq müvafiq şəxs tərəfindən mesaj sahibinin açıq açarı ilə deşifrə oluna bilər. İdentifikasiya məqsədləri üçün mesaj A kimi istinad edəcəyimiz müəllifin və ya göndərənin şəxsi açarı ilə şifrələnəcək. Bu mesaj A-nın açıq açarından istifadə edən hər kəs tərəfindən deşifrə edilə bilər. Əgər deşifrə olunan mesaj, lazımi mesajı verirsə, onda aydındır ki, mesaj həqiqətən A-nın şəxsi açarı ilə şifrələnmişdir və beləliklə, onu yalnız A göndərə bilərdi (5).

Rəqəmsal imzanın yaradılması və yoxlanılması

Sabit ölçülü mesaj xülasəsini verən mesaja heş funksiyası tətbiq edilir. İmza funksiyası rəqəmsal imza yaratmaq üçün mesaj xülasəsindən və göndərənin şəxsi açarından istifadə edir. Rəqəmsal imzanın çox sadə forması göndərənin şəxsi açarından istifadə edərək mesaj xülasəsini şifrələməklə əldə edilir. Mesaj və imza artıq alıcıya göndərilə bilər. Mesaj şifrəsizdir və hər kəs tərəfindən oxuna bilər. Bununla belə, imza göndərənin həqiqiliyini təmin edir (müvafiq orqan tərəfindən göndərilən və bir çox insanlar tərəfindən oxunmaq üçün göndərilən mesaj, mesajın həqiqiliyini təsdiq edən imza ilə). Qəbuledicidə orijinal mesaj xülasəsini bərpa etmək üçün rəqəmsal imzaya tərs imza funksiyası tətbiq edilir. Əvvəlcə rəqəmsal imza, göndərənin açıq açarı ilə deşifrələnir və mesaj xülasəsi əldə edilir. Qəbul edilmiş mesaj orijinal mesajın məruz qaldığı eyni heş funksiyasına məruz qalır. Nəticə mesaj xülasəsi imzadan əldə edilən mesaj xülasəsi ilə müqayisə edilir. Əgər onlar uyğun gəlirsə, o, mesajın həqiqətən də (iddia edilən) göndərici tərəfindən göndərilməsini və onun dəyişdirilmədiyini təmin edir (5).



Kriptoqrafik Heş funksiyası

Heş xüsusiyyəti dəyişən uzunluqlu mesajı heç bir açardan istifadə etmədən sabit uzunluqlu heş dəyərinə və ya mesaj xülasəsinə uyğunlaşdırır. Təhlükəsizlik proqramları üçün arzu olunan heş xarakteristikası kriptoqrafik heş xarakteristikası kimi tanınır ki, bu da ya əvvəlcədən unikal heş dəyəri ilə birləşdirilmiş mesajı, ya da eyni heş dəyərinə uyğun gələn mesajları tapmağı hesablama baxımından qeyri-mümkün edir. Kriptoqrafik heş xarakteristikasının birtərəfli xüsusiyyətləri və toqquşmaya davamlı xüsusiyyəti olmalıdır. Yuxarıda qeyd olunanlar ilə birlikdə, müvafiq mesajın dəyişdirilib dəyişdirilməməsinə qərar vermək üçün kriptoqrafik heş dəyəri istifadə olunur. Bununla belə, heş dəyəri qorunmalıdır. Bəzi heş funksiyaları:

- SHA-1
- SHA-224, SHA-256,
- SHA-3
- PKI (Public Key Infrasturucture – Açıq Açar İnfrastrukturu)

PKI (Açıq Açar İnfrastruktur) açıq açar şifrələmə texnologiyalarına əsaslanan açıq açar şifrələməsi və rəqəmsal imza xidmətləri təklif edən sistemdir. Əsasən kriptoqrafik nəzəriyyəyə əsaslanan və əsasən autentifikasiya və məxfilik, bütövlük xidmətlərini təqdim edən PKI, şəbəkə tətbiqində autentifikasiya və avtorizasiyanın çox vacib təhlükəsiz platformasına çevrilir və insanlara şəbəkə fəaliyyətinin informasiya təhlükəsizliyinə zəmanət verir (5; 6).

Rəqəmsal sertifikat

Rəqəmsal sertifikat Sertifikat Təşkilatı (CA - Certificate Authority) tərəfindən verilən elektron sənəddir. O, rəqəmsal imza üçün açıq açarı ehtiva edir və təşkilatın adı, açarla əlaqəli şəxsiyyəti müəyyən edir. Sertifikat açıq açarın konkret təşkilata aid olduğunu təsdiqləmək üçün istifadə olunur. ST zamin kimi çıxış edir. Rəqəmsal sertifikatlar etibarlı orqan tərəfindən verilməlidir və yalnız müəyyən bir müddət ərzində etibarlı olmalıdır. Onlar rəqəmsal imza yaratmaq üçün tələb olunur.

Rəqəmsal imzalar açıq və gizli açarlara əsaslanır. Təhlükəsizliyi təmin etmək və saxtakarlıqdan və ya zərərli istifadədən qaçmaq üçün bu açarlar qorunmalıdır. Sənədi göndərdiyiniz və ya imzaladığınız zaman sənədlərin və açarların təhlükəsiz şəkildə yaradıldığına və onların etibarlı açarlardan istifadə etdiyinə əmin olmalısınız. Etibarlı Xidmət Təchizatçısının (TSP-Trust Service Provider) bir növü olan ST-lər əsas təhlükəsizliyi təmin etmək üçün etibarlı kimi qəbul edilən və lazımi rəqəmsal sertifikatları təmin edə bilən üçüncü tərəf təşkilatlarıdır. Həm sənədi göndərən təşkilat, həm də onu imzalayan alıcı müəyyən ST-dən istifadə etməyə razı olmalıdır (9; 10).

Nəticə

Rəqəmsal İmza internet üzərindən onlayn əməliyyatlar zamanı ən təhlükəsiz məlumatlardan biridir. Rəqəmsal imza beynəlxalq ticarətdə mühüm alətə çevrilib. Digər müəssisələr də, ehtimal ki, kommersiya əməliyyatlarının artan faizində rəqəmsal imzalardan istifadə edəcəklər. Rəqəmsal imza

ənənəvi əlyazma imzanın hüquqi elementlərini təmin etdiyindən və rəqəmsal imzaların domen spesifik tətbiqindən asılı olmayaraq təkmilləşdirildiyindən, əsas diqqət həmişə autentifikasiya və məlumatların bütövlüyünün həyata keçirilməsi üzərindədir. Bundan əlavə, tədqiqatçılar tərəfindən xərcdən səmərəlilik, vaxtdan səmərəlilik, sənaye standartlarının tətbiqi, çeviklik və s. xüsusiyyətləri nəzərə alınır. Müştəri tələbləri gündən-günə artdıqca, obyekt yönümlü modelləşdirmədən istifadə edərək rəqəmsal imzaların tətbiqi üçün yeni üfüq açılacaq.

Ədəbiyyat

1. https://www.ijircst.org/DOC/7-a-comprehensive-study-on-digital-signature.pdf
2. (A Comprehensive Study on Digital Signature)
3. https://www.scirp.org/pdf/16-2.20.pdf (Research on Digital Signature Based on Digital Certificate)
4. https://www.techtarget.com/searchsecurity/definition/digital-signature
5. https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq
6. https://www.researchgate.net/publication/3227862_Digital_signatures
7. https://www.naukri.com/learning/articles/digital-signatures/
8. https://support.microsoft.com/en-us/office/digital-signatures-and-certificates-8186cd15-e7ac-4a16-8597-22bd163e8e96#__toc311530578
9. Computer Networks (Fifth Edition) Tanenbaum & Wetherall
10. https://www.signix.com/blog/what-is-a-digital-signature
11. https://www.cisa.gov/uscert/ncas/tips/ST04-018

Göndərilib: 01.02.2023 Qəbul edilib: 18.03.2023