ELEKTRON RAQAMLI IMZODAN FOYDALANISHNING AHAMIYATI

Mavlanov Aziz Bagbekovich
Jumaniyazov Munisbek Axmedjonovich
Xiva shahar Ogahiy ijod maktabi o'qituvchisi

Annotatsiya: *Ushbu maqolada Elektron imzo va Elektron raqamli imzo farqi, Elektron imzoning xususiyati, ERI olish, Elektron raqamli imzo sxemasi, Blokcheyn texnologiyasi kabi ma'lumotlar keltirilgan.*

Kalit so'zlar: *ERI, Elektron imzo, RSA, Merkle daraxtlari, Blokcheyn texnologiyasi.*

Hujjatni tasdiqlashning asosiy elementlaridan biri bu imzodir. Hujjatlarni raqamlashtirish bilan birgalikda elektron raqamli imzo (ERI) yaratildi. Bu an'anaviy imzoning muqobil varianti bo'lib, elektron hujjatlarni imzolash va haqiqiyligini tekshirishda shaxsni tasdiqlash uchun ishlatiladi. ERI vaqt va pulni sezilarli darajada tejaydi hamda ikki yil muddatga beriladi.

O'zbekiston Respublikasi Prezidenti tomonidan 2022-yil 12- oktabrdagi «Elektron raqamli imzo to'g'risida» gi O'RQ-793-son Qonun imzolandi. Hujjatga muvofiq, yuridik shaxsning ERIsi bilan tasdiqlangan elektron hujjat, quyidagi barcha shartlar mavjud bo'lganda qog'oz shaklidagi yuridik shaxsning muhri bilan tasdiqlangan hujjatga tenglashtiriladi:[1]

- Elektron raqamli imzo haqiqiyligi tasdiqlanganda;
- Elektron raqamli imzo kaliti sertifikati ERIning haqiqiyligi tasdiqlangan paytda yoki elektron hujjat imzolangan (hujjatni imzolangan vaqtini aniqlash imkoni bo'lganda) amalda bo'lganda;
- ERI uning kaliti sertifikatida ko'rsatilgan maqsadlarda foydalanilganda.

Elektron imzo va Elektron raqamli imzo ko'pincha bir-birining o'rnida ishlatiladi, ammo bu ikki tushuncha boshqacha.

Elektron Raqamli imzo raqamli shakldagi o'ziga xos xususiyat bo'lib, hujjatga o'rnatilgan barmoq izi kabi narsadir. Imzolovchi hujjat bilan bog'lanishi uchun raqamli sertifikatga ega bo'lishi kerak. Elektron raqamli imzoning yana bir muhim xususiyati shundaki, u raqamli hujjatlarni himoya qilish uchun ishlatiladi. Firibgarlar hujjatlarni elektron imzo yordamida onlayn topshirish uchun soxtalashtirishlari mumkin, ammo raqamli imzo bilan bu deyarli mumkin emas. Elektron hujjat himoyalangan; faqat vakolatli shaxs o'zgartirish yoki tahrir qilish uchun uni ko'rishi mumkin.

Elektron imzoning asosiy xususiyati shundaki, u imzolovchining hujjatni imzolash niyatini ochib beradi. Odatda u ikki tomon tarafidan tuzilgan shartnomalar yoki boshqa kelishuvlarga mos keladi. Yuqorida aytib o'tilganidek, elektron imzolarning har xil turlari mavjud. Ular barcha tomonlar o'zlarining majburiyatlarini va muayyan shartnoma tuzish niyatlarini ko'rsatganlaridan keyin qonuniy kuchga ega bo'ladilar. Elektron imzoning yana bir jihati shundaki, u hujjatning haqiqiyligini tekshirishga yordam beradi. Imzolangandan so'ng,

ishtirok etuvchi tomonlar aniqlanishi kerak. Biroq, elektron hujjatni tekshirish qiyin bo‘lishi mumkin, chunki raqamli sertifikat mavjud emas, bu jarayonni xavfsiz qiladi.[2]

ERI ni 3 ta usulda olish mumkin:

- davlat xizmatlari markazida;
- masofadan (onlayn):
- yagona interaktiv davlat xizmatlari portalida;
- ERI ro‘yxatga olish markazining rasmiy veb-saytida - e-imzo.uz.

ERI olishni istagan yuridik yoki jismoniy shaxslar Davlat soliq qo‘mitasi ro‘yxatga olish markazining rasmiy veb-saytidagi davlat xizmatidan foydalanishlari mumkin https://e-imzo.uz.[4]

Ma’lumotlardagi xatolarni aniqlash va tuzatish uchun ishlatiladi. Masalan, Hamming kodlari va Reed-Solomon kodlari. Ma’lumotlarga ortiqcha ma’lumotlarni kiritish orqali ushbu kodlar xatolarni aniqlashi va tuzatishi mumkin.

Raqamli imzolar yaxlitlik va autentifikatsiyani ta’minlash uchun assimmetrik kriptografiyadan foydalanadi. Elektron raqamli imzo jo‘natuvchining shaxsiy kaliti yordamida yaratiladi va uni jo‘natuvchining ochiq kaliti yordamida tekshirish mumkin. Agar imzo haqiqiy bo‘lsa, u ma’lumotlarning yaxlitligi va haqiqiyligini ta’minlaydi.

Merkle daraxtlari: Merkle daraxtlari, shuningdek, xesh daraxtlari sifatida ham tanilgan, katta ma’lumotlar to‘plamlarini samarali tekshirish imkonini beruvchi ma’lumotlar tuzilmalari. Ular ma’lumotlarni kichikroq bloklarga ajratadilar, har bir blok uchun xeshlarni hisoblaydilar.

Blokcheyn texnologiyasi: Dastlab Bitcoin kabi kriptovalyutalar uchun taqdim etilgan blokcheyn texnologiyasi o‘ziga xos ma’lumotlar yaxlitligi xususiyatlari tufayli turli sohalarda e’tiborni tortdi.

Blokcheyndagi har bir blok zanjirni tashkil etuvchi oldingi blokning kriptografik xeshini o‘z ichiga oladi. O‘zbekiston Respublikasining Elektron raqamli imzo to‘g‘risidagi qonunida elektron raqamli imzoga quyidagicha ta’rif berilgan:[3]

Elektron raqamli imzo oddiy qo‘lda qo‘yiluvchi imzo kabi, faqat elektron hujjatlarga qo‘yiladi va imzo qo‘yilgan Ma’lumotning yaxlitligini ta’minlaydi va imzolovchining qo‘yilgan imzodan bosh tortmasligini (rad etmasligini) kafolatlaydi. Axborot xavfsizligida rad etish muammosi mavjud, unga ko‘ra foydalanuvchi hujjatni imzolaganini rad etadi (ya’ni, men imzolamadim deb turib oladi).

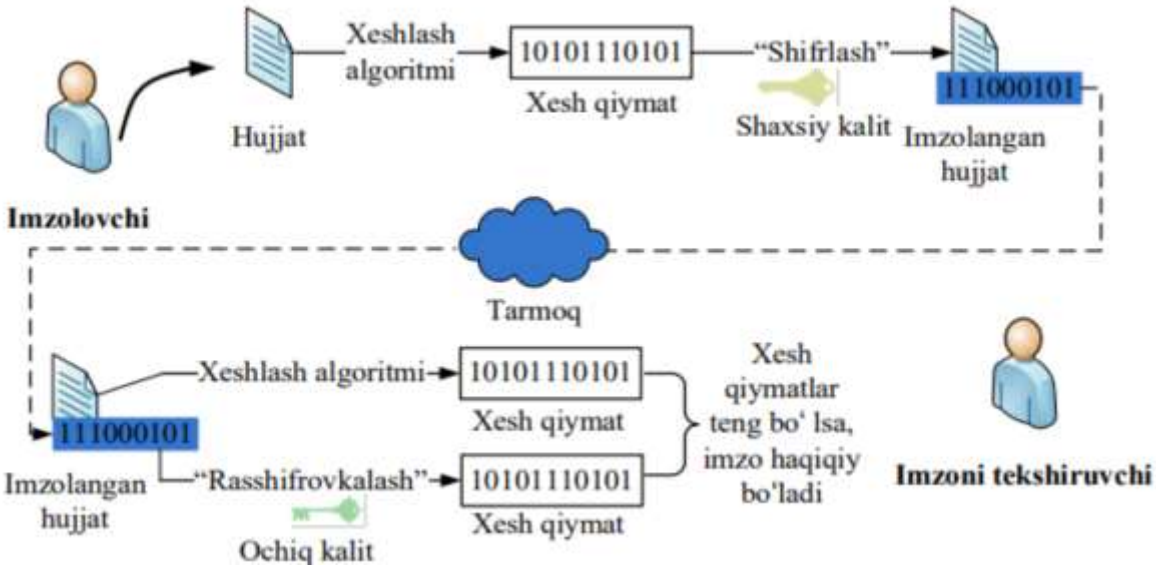
Mazkur muammoni oldini olishda aynan electron raqamli imzo tizimlaridan foydalaniladi.

Shunday qilib, ERI tizimlari nafaqat Ma’lumot yaxlitligini ta’minlaydi, balki imzolovchining majburiyatlardan tonishiga yo‘l qo‘ymaydi (yoki rad etishni oldini oladi). Shu sababli, ERI tizimlari ma’lumotlar yaxlitligini ta’minlovchi simmetrik kriptotizimlarga asoslangan MAC tizimlaridan ajralib turadi. MAC tizimlarida xesh qiymatni qayta hisoblay olmaslik uchun, matnga kalit biriktirilgan bo‘lsa , ERI tizimlarida Ma’lumotning xesh qiymati shaxsiy kaliti bilan “shifrlash” amalga oshiriladi va ERI hosil qilinadi. Ushbu xabarni “rasshifrovkalash” uchun esa tomonning ochiq kalitini bilishning o‘zi yetarli.

Demak, oddiy imzo tizimiga o‘xshash (oddiy imzo tizimida bir kishi imzo qo‘yadi va qolganlardan uning haqiqiyligini tekshirish talab etiladi).

ERI tizimida ham shaxsiy kalit egasi xabarni imzolaydi, qolganlar esa, uning ochiq kalitidan foydalanib, imzoni haqiqiyligini tekshiradi. Agar A tomon xabar *M*ga imzo qo‘ygan bo‘lsa, u holda imzo $S=[M]A$ shaklida ifodalanadi (xuddi ochiq kalitli kriptografiyada shaxsiy kalit bilan rasshifrovkalash kabi). ERI tizimlarini yaratish ikkita muolajadan iborat:

ERI ni shakllantirish va ERIni tekshirish (1-rasm).



1-rasm. Elektron raqamli imzo sxemasi

Hozirda ERI tizimini yaratishning bir nechta yo‘nalishlari mavjud. Bu yo‘nalishlarni uchta guruhga bo‘lish mumkin:

1) ochiq kalitli shifrlash algoritmlariga asoslangan;

2) simmetrik shifrlash algoritmlariga asoslangan;

3) imzoni hisoblash va uni tekshirishning maxsus algoritmlariga asoslangan raqamli imzo tizimlaridir.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. Y. A. Kuralov- Scientific Journal Impact Factor (SJIF) 2021

2.Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2001. – 376 с.

3. I.S.Olimov, X.I. Ibrohimov.Tashkent university of information technologies named after Muhammadal-Khwarizmi.Multidisciplinary Scientific Journal.ISSN: 2181-4120,VOLUME 1 | ISSUE 18.2023

4. Kheshaifaty, Nafisah, and Adnan Gutub. "Preventing multiple accessing attacks via efficient integration of captcha crypto hash functions."Int. J. Comput. Sci. Netw. Secur.(IJCSNS)20.9 (2020):

5.www.norma .uz

6.www. medium.com