INNOVATIVE PUBLICATION

Journal of Effective Learning and Sustainable Innovation

Vol.3 №1 (2025). January

innovativepublication.uz

RAQAMLI DAVRDA ISHONCHNI TA’MINLASH: ELEKTRON RAQAMLI IMZONING AHAMIYATI

Xusniddin Sotvoldiyev

Muhammad al-Xorazmiy nomidagi

Toshkent axborot texnologiyalari universiteti

Farg‘ona filiali Ta'lim sifatini nazorat qilish bo'limi

boshlig‘i, Texnika fanlari bo‘yicha falsafa doktori (PhD)

Muxammadyunus Tursunov

Dasturiy injiniring va kiberxavfsizlik

fakulteti I kurs talabasi

Annotatsiya: Ushbu maqolada raqamli imzolarning bugungi raqamli dunyodagi ahamiyati o'rganiladi. Asimmetrik kriptografiya va ochiq kalitlar infratuzilmasi asosida ish ko’rish raqamli imzolar egalarining haqiqiyligini tekshirish, hujjatlarning yaxlitligini ta’minlash va rad etishning oldini olish orqali xavfsizlikni ta’minlashi haqida so’z yuritiladi. Menejment muammolari yoki ehtimoliy tahdidlar mavjud bo'lsa-da, blokcheyn texnologiyasi, post-kvant kriptografiyasi va sun'iy intellekt kabi texnologiyalar orqali raqamli imzolardan xavfsiz ravishda foydalanish mumkinligiga ham to’xtab o’tiladi.

Kalit so’zlar: Raqamli imzo autentifikatsiyasi, Hujjat yaxlitligini tekshirish, Rad etmaslik texnologiyasi, Assimetrik kriptografiyani amalga oshirish, PKI xavfsizlik

standartlari, X.509 sertifikatini boshqarish, eIDAS me’yorlariga muvofiqligi, Blokcheyn, Raqamli imzo, Kvant kriptografiyasi.

Kirish

Jamiyatlar raqamli platformalarga tobora ko‘proq tayanib, muloqot, savdo va hamkorlikni onlayn tarzda amalga oshirar ekan, hujjat va xabarlarda ishtirokchilarning shaxsini hamda hujjatning haqiqiyligini tasdiqlash zarurati hech qachon hozirgi paytdagidek muhim masala bo‘lmagan. Elektron raqamli imzolar aynan shu ehtiyojni qondirishda asosiy yechim sifatida maydonga chiqdi. An’anaviy qo‘l imzolari ko‘rish orqali tekshirilsa, oddiy elektron imzolar esa shunchaki terilgan ism yoki skaner qilingan tasvir bo‘lishi mumkin.

Raqamli imzolar esa murakkab kriptografik protokollardan foydalanadi, bu esa hujjatning o‘zgartirilmaganligini va uni imzolagan shaxsga chinakam bog‘liqligini kafolatlaydi. Moliyaviy shartnomalar va ish bitimlaridan tortib davlat xizmatlarigacha bo’lgan onlayn tranzaksiyalar tez sur’atlar bilan o‘sar ekan, raqamli imzo ishonch poydevori sifatida maydonga chiqmoqda. U shubhalarni kamaytiradi, firibgarlikni cheklaydi va globallashgan raqamli makonda xavfsiz hamkorlik qilish uchun zarur bo‘lgan ishonch muhitini shakllantiradi.

Asosiy xususiyatlar va texnik asoslar

“Elektron raqamli imzo — elektron hujjatdagi mazkur elektron hujjat axborotini elektron raqamli imzoning yopiq kalitidan foydalangan holda maxsus o‘zgarishlar natijasida hosil qilingan hamda elektron raqamli imzoning ochiq kaliti yordamida elektron hujjatdagi axborotda xatolik mavjud emasligini aniqlash va elektron raqamli imzo kalitining egasini identifikatsiya qilish imkonini beradigan imzo”[1] deb ta’rif beriladi O‘zbekiston Respublikasining “Elektron raqamli imzo” to‘g‘risidagi qonunida.

Raqamli imzolar asimmetrik kriptografiya va Ochiq Kalit Infratuzilmasi (PKI) tamoyillariga asoslanadi. Bu tizimda har bir foydalanuvchi takrorlanmas ikki kalitga ega: shaxsiy kalit (maxfiy saqlanadi) va ochiq kalit (boshqalarga ham ulashiladi). Imzo qo‘yuvchi hujjatni xeshlash algoritmi orqali qayta ishlaydi va natijada o‘ziga xos, qat’iy uzunlikka ega xesh-hisob hosil bo‘ladi. Shaxsiy kalit yordamida shu xesh shifrlanadi. Qabul qiluvchi tomon hujjatni olgach, imzo qo‘yuvchining ochiq kaliti bilan xeshni shifrdan chiqaradi va hujjatni yana bir bor xeshlab, ikki xeshni solishtiradi. Agar ular mos kelsa, hujjat o‘zgarmagan va imzo qo‘yuvchining shaxsi tasdiqlangan bo‘ladi [2].

Raqamli imzolarning afzalliklari uchta asosiy xususiyatda namoyon bo‘ladi. Birinchisi, autentifikatsiya – imzo qo‘ygan shaxsning haqiqiyligini tasdiqlaydi. Ikkinchisi, butunlik (integritet) – hujjat imzo qo‘yilganidan keyin o‘zgartirilgan bo‘lsa, imzo bekor bo‘lishini ta’minlaydi. Uchinchi xususiyat, inkor eta olmaslik (non-repudiation) – imzo qo‘ygan shaxsga keyinchalik o‘z imzosini inkor eta olmasligini ta’minlaydi. [3] O’zarov muvofiqlik va keng qabul qilinishni ta’minlash maqsadida, X.509 kabi xalqaro standartlar [6] ochiq kalitlar va raqamli sertifikatlarni berish hamda boshqarishda umumiy mezonlarni joriy etadilar.

Foydalar va ahamiyati

Raqamli imzolar raqamli ekotizimlarda xavfsizlikni sezilarli darajada kuchaytiradi, hujjatlarni buzish, qalbakilashtirish yoki kimlikni soxtalashtirish imkoniyatlarini kamaytiradi. Ular hujjat va xabarlar tranzit jarayonida o‘zgartirilmaganligini kafolatlab, ayniqsa moliya, sog‘liqni saqlash va huquq kabi sohalarda ma’lumotlarning butunligi va maxfiyligini ta’minlaydi.

Operatsion nuqtayi nazardan, raqamli imzolar ilgari qog‘ozga asoslangan ish jarayonlariga bog‘liq bo‘lgan bosqichlarni osonlashtiradi. Endi hujjatlarni chop etish, imzolash, skanerlash va pochta orqali yuborish shart emas. Tomonlar hujjatlarni darhol

imzolab, almashishlari mumkin, natijada xarajatlar kamayadi, jarayonlar tezlashadi hamda qog‘oz iste’molini qisqartirish orqali ekologik ta’sir ham ijobiy tomonga o‘zgaradi. Bu tezkor va o‘zgaruvchan global bozorda raqobatbardoshlikni saqlashga intilayotgan tashkilotlar uchun juda muhimdir.

Bundan tashqari, raqamli imzolar transchegaraviy tranzaksiyalarni xavfsiz amalga oshirishga yordam beradi. Yevropa Ittifoqining eIDAS Reglamenti [4] yoki AQShning ESIGN Qonuni [5] kabi huquqiy normalar raqamli imzolarga qo‘l imzosiga teng huquqiy kuch beradi. Bu hujjatlarning huquqiy jihatdan tan olinishi va sudlarda dalil sifatida qabul qilinishini kafolatlaydi. Natijada tashkilotlar xalqaro bitimlarni osongina tuzishlari, chet el mijozlari bilan shartnomalarni mustahkamlashlari va raqamli yozuvlardan huquqiy isbot sifatida foydalanishlari mumkin. Shu tariqa raqamli imzolar global miqyosda ishonch va obro‘ni mustahkamlaydi, iqtisodiy o‘sish va xizmat ko‘rsatish almashinuvini kuchaytiradi.

Muammolar va kelajakka nazar

Ko‘plab afzalliklariga qaramasdan, raqamli imzolar ayrim muammolarga duch kelishi mumkin. Kalitlarning buzilishi, kriptografik algoritmlardagi zaifliklar yoki foydalanuvchi xatolari tizim ishonchliligini kamaytirishi mumkin. Ushbu xavf-xatarlarni bartaraf etish uchun doimiy ravishda xodimlar va foydalanuvchilarni o‘qitish, kuchli kiberxavfsizlik choralari ko‘rish va kriptografik standartlarni muntazam ravishda yangilash lozim. Shuningdek, foydalanuvchilarning texnologiyani qabul qilishlari uchun dastlabki shubha va o‘rganish jarayonlarini yengish zarur bo‘ladi.

Texnologiyalar rivojlanishi bilan raqamli imzo tizimlari ham takomillashishi kerak. Blokcheyn asosidagi identifikatsiya yechimlari va post-kvant kriptografiya tadqiqotlari kelajakda raqamli imzo mustahkamligini yangi bosqichga ko‘tarishi kutilmoqda. Kvant hisoblash qudrati ortar ekan, kriptograflar kvant hujumlariga bardoshli algoritmlarni ishlab

chiqmoqdalar. Shu bilan birga, sun’iy intellekt va tarqoq daftar texnologiyalari raqamli imzo jarayonlarida qo‘llanilishi yoki yangi murakkabliklarni yuzaga keltirishi mumkin. Innovatsiya va doimiy takomillashtirish raqamli imzolarni raqamli dunyoda ishonchli poydevor sifatida saqlab turadi.

Xulosa

Raqamli imzolar tobora raqamli tus olayotgan dunyoda xavfsizlik, haqiqiylik va samaradorlikni ta’minlovchi asosiy mexanizmdir. Imzo qo‘yuvchini tasdiqlash, hujjat butunligini saqlash va inkor eta olmaslikni kafolatlash orqali ular ishonchli onlayn hamkorlik va savdoni qo‘llab-quvvatlaydi. Raqamli imzolar vaqtni tejash, xarajatlarni kamaytirish, huquqiy talablarga javob berish va globallashgan iqtisodiy muhitda imkoniyatlar yaratish orqali beqiyos ahamiyat kasb etadi. Onlayn tranzaksiyalar sur’ati oshib borar ekan, kriptografik vositalarni rivojlantirish, huquqiy mezonlarni mustahkamlash va foydalanuvchilarning xabardorligini oshirish kelajakda ham raqamli imzolarni raqamli ishonch garovi sifatida saqlab qolishga yordam beradi.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasining Qonuni. 12.10.2022 yildagi O‘RQ-793-son.
2. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1997). Amaliy Kriptografiya qo’llanmasi.
3. NIST. (2013). Raqamli Imzo Standartlari (RIS) (FIPS PUB 186-4). Standartlar va texnologiya instituti
4. Yevropa parlamenti va kengashi. (2014). Qonunlar (EU) No 910/2014 (eIDAS). Yevropa ittifoqining rasmiy jurnali.
5. AQSH. (2000). Global va milliy savdo qonunida elektron imzolar (ESIGN Act).
6. ITU-T. (2019). Tavsiya X.509: Axborot texnologiyalari - Ochiq tizimlarning o'zaro bog'lanishi - Katalog: Ochiq kalit va atribut sertifikatlari freymvorklari.