

ELEKTRON TO'LOV TIZIMLARIDA TOKENIZATSIYA TEXNOLOGIYASINING AHAMIYATI

*Farg'ona davlat texnika universiteti
681-23 guruh talabasi
Iqboljon G'aniyev Ibrohimjon o'g'li*

Annotatsiya: Ushbu maqolada elektron to'lov tizimlarida xavfsizlikni ta'minlashda tokenizatsiya texnologiyasining o'rni va ahamiyati tahlil qilinadi. Tokenizatsiya jarayonining ishlash mexanizmi, an'anaviy shifrlash usullari bilan farqlari hamda elektron to'lovlarda firibgarlik xavfini kamaytirishdagi roli yoritib beriladi. Shuningdek, PCI DSS standarti talablariga muvofiqlikni ta'minlashda tokenizatsiya texnologiyasining afzalliklari ko'rib chiqiladi.

Kalit so'zlar: Elektron to'lov tizimlari, tokenizatsiya, PCI DSS, tranzaksiya, axborot xavfsizligi, bank kartalari.

Annotation: In this article, the role and importance of tokenization technology in ensuring security in electronic payment systems are analyzed. The mechanism of the tokenization process, its differences from traditional encryption methods, and its role in reducing fraud risks in electronic payments are discussed. In addition, the advantages of tokenization technology in ensuring compliance with PCI DSS requirements are examined.

Keywords: Electronic payment systems, tokenization, PCI DSS, transaction security, information security, bank cards.

Аннотация: В данной статье анализируется роль и значение технологии токенизации в обеспечении безопасности электронных платёжных систем. Рассматривается механизм работы процесса токенизации, его отличия от традиционных методов шифрования, а также роль в снижении рисков мошенничества при электронных платежах. Кроме того, изучаются преимущества технологии токенизации в обеспечении соответствия требованиям стандарта PCI DSS.

Ключевые слова: Электронные платёжные системы, токенизация, PCI DSS, безопасность транзакций, информационная безопасность, банковские карты.

Kirish

Elektron to'lov tizimlarining rivojlanishi

So'nggi yillarda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi elektron to'lov tizimlarining keng ommalashishiga olib keldi. Bank kartalari, mobil ilovalar, internet-banking va raqamli hamyonlar orqali to'lovlarni amalga oshirish

kundalik hayotning ajralmas qismiga aylandi. Elektron to'lov tizimlari naqd pulsiz hisob-kitoblarni tezkor va qulay tarzda amalga oshirish imkonini berib, iqtisodiyotning raqamlashtirilishiga xizmat qilmoqda.

To'lovlarda xavfsizlik muammolari

Elektron to'lov tizimlarining rivojlanishi bilan bir qatorda, axborot xavfsizligi muammolari ham dolzarb bo'lib bormoqda. Karta ma'lumotlarining noqonuniy qo'lga kiritilishi, firibgarlik holatlari va kiberhujumlar elektron to'lov tizimlari uchun asosiy tahdidlar hisoblanadi. Ayniqsa, haqiqiy karta ma'lumotlarining ochiq holda saqlanishi va uzatilishi xavfsizlik darajasini pasaytiradi hamda moliyaviy yo'qotishlarga olib kelishi mumkin.

Tokenizatsiya tushunchasining paydo bo'lishi

Mazkur muammolarni bartaraf etish maqsadida elektron to'lov tizimlarida zamonaviy xavfsizlik texnologiyalari joriy etila boshlandi. Shulardan biri — **tokenizatsiya texnologiyasi** hisoblanadi. Tokenizatsiya jarayonida haqiqiy karta ma'lumotlari maxsus token bilan almashtiriladi, bu esa to'lov jarayonida karta ma'lumotlarining oshkor bo'lish ehtimolini kamaytiradi. Natijada, elektron to'lov tizimlarida xavfsizlik darajasi oshib, foydalanuvchilar uchun ishonchli to'lov muhiti yaratiladi

1. Elektron to'lov tizimlarining umumiy tavsifi

Elektron to'lov tizimi tushunchasi

Elektron to'lov tizimi — bu moliyaviy operatsiyalarni axborot-kommunikatsiya texnologiyalari yordamida amalga oshirishni ta'minlovchi tizimlar majmuasidir. Ushbu tizimlar bank kartalari, mobil ilovalar, internet-banking va raqamli hamyonlar orqali naqd pulsiz to'lovlarni amalga oshirish imkonini beradi. Elektron to'lov tizimlarining asosiy vazifasi to'lov jarayonlarini tezkor, qulay va xavfsiz tarzda bajarishdan iborat.

Zamonaviy elektron to'lov tizimlari savdo nuqtalari, banklar va mijozlar o'rtasida real vaqt rejimida axborot almashuvini ta'minlab, to'lovlarning aniqligi va shaffofligini oshiradi. Natijada, naqd pulga bo'lgan ehtiyoj kamayib, iqtisodiy operatsiyalar samaradorligi ortadi.

POS-terminal, to'lov shlyuzi va banklararo aloqa

POS-terminal (Point of Sale) — savdo nuqtalarida to'lovlarni qabul qilish uchun mo'ljallangan elektron qurilma bo'lib, bank kartalari orqali amalga oshiriladigan tranzaksiyalarni qayta ishlaydi. POS-terminal karta ma'lumotlarini o'qib, to'lov summasini shakllantiradi va uni to'lov tizimiga uzatadi. To'lov shlyuzi (payment gateway) esa savdo nuqtasi yoki onlayn do'kon bilan bank tizimi o'rtasida vositachi vazifasini bajaradi. U to'lov ma'lumotlarini shifrlash, autentifikatsiya qilish va tranzaksiyani bank tizimlariga xavfsiz uzatishni ta'minlaydi. Banklararo aloqa esa to'lov jarayonining muhim bo'g'ini hisoblanib, unda ekvayer bank, to'lov tizimi va

emitent bank o'rtasida axborot almashuvi amalga oshiriladi. Ushbu aloqa orqali tranzaksiya tekshiriladi va uning bajarilishi yoki rad etilishi bo'yicha qaror qabul qilinadi.

Naqd pulsiz to'lovlarning afzalliklari

Naqd pulsiz to'lovlar iqtisodiyotning raqamlashtirilishida muhim o'rin tutadi. Ularning asosiy afzalliklaridan biri — to'lov jarayonining tezkorligi va qulayligidir. Mijozlar to'lovlarni bir necha soniya ichida amalga oshirish imkoniyatiga ega bo'ladi. Shuningdek, naqd pulsiz to'lovlar moliyaviy xavfsizlikni oshiradi, chunki katta miqdordagi naqd pul muomalasi kamayadi. Bunda to'lovlar elektron tarzda qayd etilib, firibgarlik holatlarini aniqlash va nazorat qilish imkoniyati kengayadi. Bundan tashqari, naqd pulsiz to'lovlar davlat byudjeti tushumlarining shaffofligini ta'minlab, soliq tizimi samaradorligini oshiradi.

2. Tokenizatsiya texnologiyasining mohiyati

Token va haqiqiy karta ma'lumotlari (PAN) farqi

Tokenizatsiya — bu elektron to'lov tizimlarida **karta ma'lumotlarini (Primary Account Number – PAN) xavfsizroq tarzda saqlash va uzatish** texnologiyasidir. Tokenizatsiyada haqiqiy karta raqami o'rniga **token** deb ataladigan tasodifiy yoki maxsus kod ishlatiladi.

Masalan:

Haqiqiy karta raqami (PAN): 8600 1234 5678 9012

Token: TKN-9F3A-77X2

Shu tarzda, tokenni o'g'irlash orqali haqiqiy karta ma'lumotlariga kira olish imkoni yo'q, chunki token ma'lumotlari faqat maxsus tizimlarda haqiqiy karta bilan bog'liq bo'ladi.

Tokenizatsiya qanday ishlaydi

Tokenizatsiya jarayoni quyidagi bosqichlarda amalga oshadi:

1. **Ma'lumot yuborish** – mijoz POS-terminal yoki onlayn to'lov sahifasida karta ma'lumotlarini kiritadi.
2. **Token yaratish** – karta raqami tokenizatsiya serveriga uzatiladi, u yerda token yaratiladi.
3. **Tokenni saqlash** – merchant tizimi tokenni saqlaydi, haqiqiy karta raqami esa xavfsiz serverda (token vault) saqlanadi.
4. **Tranzaksiya amalga oshirish** – to'lov yuborilganda token orqali haqiqiy karta aniqlanadi va tranzaksiya bajariladi.

Tokenizatsiya jarayoni ma'lumotlarning xavfsiz uzatilishini ta'minlaydi va firibgarlik xavfini sezilarli darajada kamaytiradi.

Token vault tushunchasi

Token vault — bu haqiqiy karta ma'lumotlarini xavfsiz saqlashga mo'ljallangan server yoki ma'lumotlar bazasi.

Faqat tokenizatsiya tizimi orqali tokenlar bilan bog'liq haqiqiy ma'lumotlarga kirish mumkin.

Token vault ma'lumotlar xavfsizligini oshirib, PCI DSS talablariga muvofiq ishlashni ta'minlaydi.

Shu orqali, merchant tizimlari nafaqat tranzaksiyalarni amalga oshiradi, balki mijozlar karta ma'lumotlarini saqlashda xavfsiz bo'ladi.

Tokenizatsiya va token vault yordamida elektron to'lov tizimlari zamonaviy xavfsizlik talablari bilan moslashadi va firibgarlikning oldini samarali oladi.

3. Tokenizatsiya asosida tranzaksiya jarayoni

Mijoz → Merchant → Tokenizatsiya xizmati

Tokenizatsiya asosidagi to'lov jarayoni bir necha bosqichda amalga oshadi. Avvalo, mijoz POS-terminal yoki onlayn to'lov sahifasida karta ma'lumotlarini kiritadi. Ushbu ma'lumotlar **merchant** tizimiga uzatiladi. Merchant esa haqiqiy karta raqamlarini saqlamaydi, balki **tokenizatsiya xizmatiga** yuboradi. Tokenizatsiya xizmati haqiqiy karta raqamini token bilan almashtiradi va merchantga faqat tokenni qaytaradi.

Token orqali tranzaksiyani amalga oshirish

Merchant token va to'lov summasini **to'lov shlyuziga** yuboradi. Shlyuz esa tokenni tekshiradi va tranzaksiyani bank tizimiga uzatadi. Bank tizimi token orqali haqiqiy karta ma'lumotini aniqlaydi va mablag' yetarliligini tekshiradi. Agar tranzaksiya muvaffaqiyatli bo'lsa, javob kodi (masalan, 00) qaytariladi. Agar mablag' yetarli bo'lmasa yoki karta bloklangan bo'lsa, rad etish kodi (51 yoki 05) beriladi.

Detokenizatsiya jarayoni

Detokenizatsiya — token orqali haqiqiy karta ma'lumotini qayta tiklash jarayonidir. Ushbu jarayon faqat tokenizatsiya serveri yoki token vault orqali amalga oshiriladi. Merchant tizimi yoki uchinchi tomon ushbu jarayonni amalga oshira olmaydi.

Detokenizatsiya quyidagi vazifalarni bajaradi:

1. Tranzaksiya jarayonida tokenni haqiqiy karta bilan bog'lash
2. Tranzaksiya xavfsizligini ta'minlash
3. Firibgarlik holatlarini aniqlash va oldini olish

Tokenizatsiya va detokenizatsiya jarayonlari birgalikda elektron to'lov tizimlarida ma'lumotlarni himoya qilish va firibgarlik xavfini sezilarli darajada kamaytiradi.

4. Tokenizatsiya va shifrlash texnologiyalarini taqqoslash

Shifrlashning kamchiliklari

Shifrlash — ma'lumotlarni maxfiylashtirish va uzatishda xavfsizlikni ta'minlashning an'anaviy usuli hisoblanadi. Shifrlash jarayonida ma'lumotlar maxfiy kalit yordamida kodlanadi va faqat kalitni bilgan shaxs yoki tizim tomonidan tiklanadi. Biroq, shifrlashning ba'zi kamchiliklari mavjud:

1. **Ma'lumotlarning oshkor bo'lish xavfi** – agar kalit o'g'irlangan bo'lsa, barcha ma'lumotlar xavf ostida qoladi.
2. **Murakkab boshqaruv** – ko'p tranzaksiya va tizimlarda kalitlarni xavfsiz saqlash va yangilash qiyin.
3. **Ishlash samaradorligi** – katta hajmdagi ma'lumotlarni shifrlash va deshifrlash tizim resurslarini ko'p talab qiladi.

Tokenizatsiyaning ustun tomonlari

Tokenizatsiya ma'lumotlarni shifrlashga alternativ sifatida ishlatiladi va bir qator afzalliklarga ega:

- 1.**Haqiqiy ma'lumotlarning oshkor bo'lmashligi** – merchant tizimlarida faqat token saqlanadi, haqiqiy karta raqamlari xavfsiz serverda saqlanadi.
- 2.**Firibgarlik xavfini kamaytirish** – o'g'irlangan tokenni ishlatib haqiqiy karta ma'lumotlariga kira bo'lmaydi.
- 3.**PCI DSS talablariga moslik** – tokenizatsiya tizimlari kartani saqlash va uzatishda xavfsizlik standartlariga javob beradi.
- 4.**Resurslarni tejash** – tokenlar kichik va statik bo'lgani uchun tizim resurslariga yuk kamayadi.

Qaysi holatda qaysi texnologiya ishlatiladi

Shifrlash:

Banklararo tizimlarda, tranzaksiya uzatish vaqtida ma'lumotlarni himoya qilishda

Katta hajmdagi ma'lumotlarni xavfsiz saqlashda

Tokenizatsiya:

Merchant va onlayn do'konlarda karta ma'lumotlarini saqlashda

Firibgarlik xavfini kamaytirish va PCI DSS talablarini bajarishda

Mobil ilovalar va raqamli hamyonlarda xavfsiz tranzaksiya ta'minlashda

Tokenizatsiya va shifrlash bir-birini to'ldiruvchi texnologiyalar bo'lib, zamonaviy elektron to'lov tizimlarida xavfsizlikni maksimal darajada oshirish uchun birgalikda ishlatiladi.

5. Tokenizatsiyaning elektron to'lov tizimlaridagi afzalliklari

Karta ma'lumotlari oshkor bo'lmashligi

Tokenizatsiya texnologiyasining eng muhim afzalliklaridan biri — haqiqiy karta ma'lumotlarining (PAN) ochiq holda saqlanmasligidir. Elektron to'lov jarayonida merchant tizimlari faqat token bilan ishlaydi, haqiqiy karta raqamlari esa maxsus himoyalangan token vault'da saqlanadi. Natijada, ma'lumotlar bazasiga ruxsatsiz kirish holatlarida ham karta ma'lumotlarining oshkor bo'lish ehtimoli keskin kamayadi.

Firibgarlik xavfining kamayishi

Tokenizatsiya firibgarlik holatlarining oldini olishda samarali mexanizm hisoblanadi. Token haqiqiy karta ma'lumotlariga to'g'ridan-to'g'ri bog'lanmaganligi sababli, uni noqonuniy qo'lga kiritish orqali moliyaviy operatsiyalarni amalga oshirish imkoniyati deyarli mavjud emas. Bu esa elektron to'lov tizimlarida mijozlar ishonchini oshirib, xavfsizlik darajasini sezilarli darajada kuchaytiradi.

PCI DSS talablariga moslik

PCI DSS (Payment Card Industry Data Security Standard) standarti bank kartalari bilan ishlovchi tizimlar uchun qat'iy xavfsizlik talablarini belgilaydi. Tokenizatsiya texnologiyasidan foydalanish orqali merchantlar haqiqiy karta ma'lumotlarini saqlash zaruratidan xalos bo'ladi. Bu esa PCI DSS talablarini bajarishni soddalashtiradi, audit jarayonlarini yengillashtiradi va xavfsizlik bilan bog'liq xarajatlarni kamaytiradi.

Onlayn va mobil to'lovlar xavfsizligi

Zamonaviy onlayn va mobil to'lov tizimlarida tokenizatsiya muhim rol o'ynaydi. Mobil ilovalar va raqamli hamyonlarda tokenlardan foydalanish foydalanuvchi ma'lumotlarini himoya qilish bilan birga, tezkor va qulay to'lovlarni ta'minlaydi. Shu orqali, tokenizatsiya texnologiyasi elektron savdo va mobil banking tizimlarida xavfsizlikni ta'minlashning ajralmas qismiga aylanadi.

Xulosa

Tokenizatsiyaning zamonaviy to'lov tizimlaridagi ahamiyati

Mazkur maqolada elektron to'lov tizimlarida tokenizatsiya texnologiyasining ahamiyati atroflicha tahlil qilindi. Tokenizatsiya texnologiyasi haqiqiy karta ma'lumotlarini himoyalash orqali to'lov jarayonlarida xavfsizlik darajasini sezilarli darajada oshiradi. Ushbu texnologiya yordamida karta ma'lumotlarining oshkor bo'lishi, firibgarlik holatlari va moliyaviy xavflar minimallashtiriladi. Shuningdek, tokenizatsiya elektron to'lov tizimlarida PCI DSS kabi xalqaro xavfsizlik standartlariga moslikni ta'minlashda muhim o'rin tutadi.

Kelajakda tokenizatsiya texnologiyasining rivojlanish istiqbollari

Kelajakda tokenizatsiya texnologiyasi elektron to'lov tizimlarining ajralmas qismiga aylanishi kutilmoqda. Mobil to'lovlar, raqamli hamyonlar va onlayn savdo hajmining oshishi tokenizatsiyaga bo'lgan ehtiyojni yanada kuchaytiradi. Shuningdek, sun'iy intellekt va biometrik autentifikatsiya texnologiyalari bilan integratsiya qilinishi tokenizatsiyaning imkoniyatlarini kengaytirib, to'lov tizimlarining xavfsizligini yangi bosqichga olib chiqadi. Natijada, tokenizatsiya texnologiyasi kelgusida elektron to'lov tizimlarining barqaror va ishonchli ishlashini ta'minlovchi asosiy texnologiyalardan biri bo'lib qoladi.

Foydalanilgan adabiyotlar

1.PCI Security Standards Council.

PCI DSS Quick Guide: Understanding the Payment Card Industry Data Security

Standard. Wakefield, MA, USA, 2022.

2.PCI Security Standards Council.

Payment Card Industry Data Security Standard (PCI DSS), Version 4.0.
PCI SSC, 2022.

3.Visa Inc.

Visa Token Service – Tokenization Best Practices and Implementation Guide.
Visa Developer Documentation, 2021.

4.Mastercard Incorporated.

Mastercard Digital Enablement Service (MDES) – Tokenization Overview.
Mastercard Developers Documentation, 2021.

5.Stallings, W.

Cryptography and Network Security: Principles and Practice.
7th Edition, Pearson Education, 2017.