ONLINE BANK TIZIMLARIDA FOYDALANUVCHILARNI QR KOD ASOSIDA MOBILE-OTP ORQALI AUTENTIFIKATSIYALASH

Mardiyev Ulugbek Rasulovich
Muhammad al-Xorazmiy nomidagi TATU, katta o‘qituvchi
twofine@mail.ru

ANNOTATSIYA

Onlayn bank tizimlarida foydalanuvchilarni autentifikatsiya qilish onlayn-banking xizmatlarining xavfsizligi va ishonchliligini ta’minlashning muhim jarayonidir. Autentifikatsiya jarayoni odatda foydalanuvchining identifikatorini foydalanuvchi nomi va parol, xavfsizlik belgilari, biometrik tekshirish va boshqa usullar kabi bir yoki bir nechta omillar orqali tekshirishni o‘z ichiga oladi. Xavfsizlik va qulaylikni muvozanatlash onlayn-bank tizimlari uchun muhim muammo hisoblanadi. Ushbu maqolada online bank tizimlarida foydalauvchilarni autentifikatsiyalashda QR kod asosida mobile-OTP orqali autentifikatsiyalash usuli taklif etilgan.

Kalit so‘zlar: *QR kod, OTP, autentifikatsiyalash, online bank tizimlari.*

KIRISH

Bank tizimida foydalanuchilarning pul tranzaksiyalari va pul bilan bog‘liq bo‘lgan ma’lumotlari saqlanganligi bois, tashkilotning ushbu ma’lumotlarini himoyalashda axborot xavfsizligiga jiddiy yondashishi talab etiladi. Foydalanuvchilarni autentifikatsiyalash axborot xavfsizligini ta’minlashning birlamchi vositasi hisoblanadi. Foydalanuvchilarni autentifikatsiyalashning bir nechta usullari mavjud. Bular foydalanuchilarning login va parolidan tortib biometrik autentifikatsiyagacha. Axborot texnologyalarining jadal suratlarda rivojlanishi bank tizimlarining axborotlarni himoyalashda zamon talablariga moslashishiga majbur etadi. Xar bir bank uchun umumiy bo‘lgan to‘g‘ri keladigan autentifikatsiya texnologiyasini tanlab bo‘lmaydi [1].

Onlayn bank tizimlarida autentifikatsiyalashning maqsadi Internet orqali bank hisoblariga xavfsiz kirishni ta’minlash uchun mo‘ljallangan. Bugungi raqamli asrda onlayn-bank tizimlarining qulayligi va foydalanuvchanligi tufayli tobora ommalashib bormoqda. Biroq, bu qulaylik bilan bank hisoblari va maxfiy shaxsiy ma’lumotlarga ruxsatsiz kirish xavfi mavjud. Onlayn bank tizimlarida autentifikatsiyalash foydalanuvchining shaxsini tekshirishning xavfsiz va ishonchli vositalarini taqdim etish orqali ushbu xavfni bartaraf etishga qaratiladi [2].

Milliondan ziyod internet foydalanuvchilari har kuni serverga kirishga ruxsat oladi. Ushbu serverlardan ko‘p qismi foydalanish uchun ochiq hisoblanadi. Ular foydalanuvchilarga xizmatlardan foydalanishga ruxsat beradi. Masalan google.com serveri foydalanuvchilarni identifikatsiya qilmasdan ularga izlash xuquqini beradi. Shunday holatlar ham borki bunda kompaniya qaysi foydalanuvchilarning xizmatlardan foydalanish huquqi borligini kuzatib boradi. Bank kompaniyalari foydalanuvchilarning muhim resurslarga kirishidan oldin ularni tasdiqlashi kerak bo‘lgan tashkilotlarning eng yaxshi namunasidir. Banklar autentifikatsiya jarayonini jiddiy qabul qilishi kerak bo‘lgan tashkilotdir [3]. Bank muhim shaxsiy identifikatsiyalovchi ma’lumotlarni saqlovchi hisoblanadi. Ushbu ma’lumotlarga quyidagilar kiradi: ijtimoiy sug‘urta nomeri, yashash manzili, telefon nomeri, elektron pochta manzili, hisob nomerlari, kreditlar tarixi va boshqa mijozlar va ishchilarning ma’lumotlari [4].

Hozirgi kunda autentifikatsiyalashni ko‘plab usullari mavjud bo‘lib, quyida keltirilgan jadvalda ularning tahlili keltirilgan (1-jadval).

1-jadval

Autentifikatsiyalash usullari klasifikatsyaisi

Bilish asosidagi autentifikatsiya	**Egalik qilish asosidagi autentifikatsiya**	**Hatti karakatlariga asoslangan autentifikatsiya**	**Biologik parametrlariga asoslangan autentifikatsiya**
parollar	magnit kartalar	tovush signali	barmoq izi
pin kod	usb tokenlar	imzolar	qo‘l geometriyasi
identifikatsiyalanuvchi rasmlar	one time passwords	klaviatura tugmalarini bosish ritmi	ko‘z xususiyatlari

ONLINE BANK TIZIMINI QR KOD BILAN MOBILE-OTP ORQALI AUTENTIFIKATSIYALASH

QR kodlar oddiy maxsulotlarning yorlig‘iga qo‘yiladigan shtrix kodlarning ikki o‘lchovli ko‘rinishi hisoblanadi. Boshida QR kodlar avtomobilqurilishda logistika jarayonlarini optimizatsiyalash uchun ishlatilgan, lekin smartfonlarning keng tarqalishi natijasida QR kodlar marketingda keng qo‘llanilib boshladi. QR “Quick Response” – tezkor javob ma’nosini anglatib, kodda yashiringan ma’lumotni darhol olishni amalga oshiradi. QR kodlar ochiq texnologiya bo‘lganliki bilan mashhurlikka ega bo‘lib, ixtiyoriy inson foydalanishi mumkin. Odatdagi shtrix kodlardan ustun va afzalligi axborot xajmining ko‘pligida va zararga chidamligidadir [5].

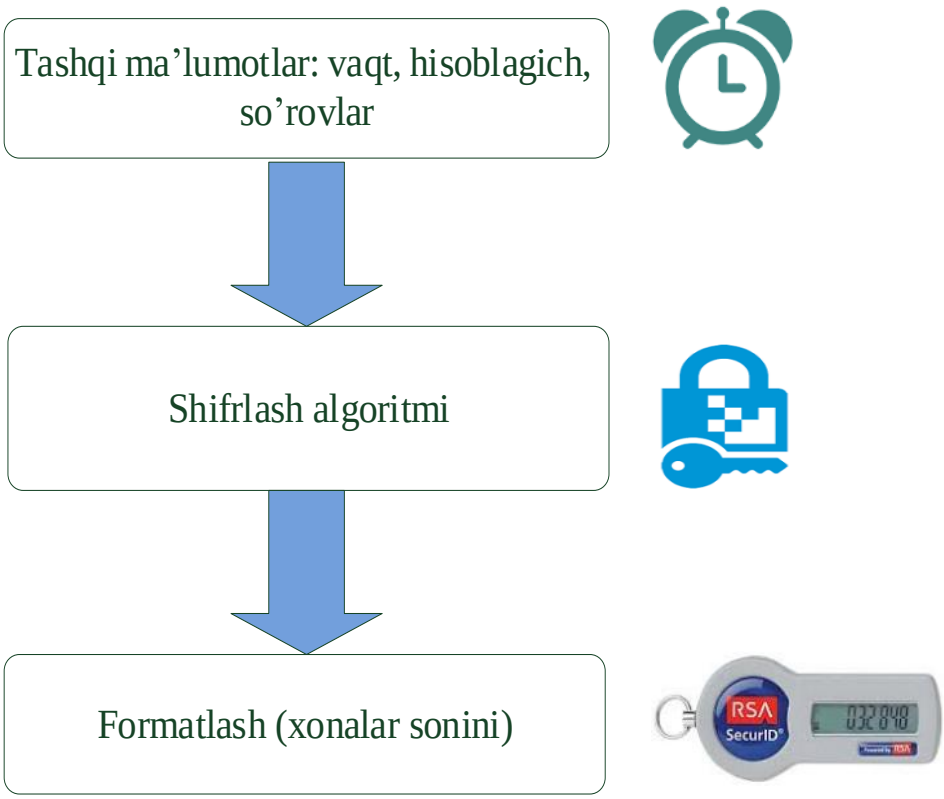
OTP (One time passwords) – dinamik autentifikatsion ma’lumot bo‘lib, har xil yo‘llar orqali generatsiya qilinib bir marta ishlatish uchun yaratiladi [6].

Parollarni generatsiya tokenlardan foydalanadi. OTP tokenlar – mobil shaxsiy qurilma bo‘lib, ma’lum foydalanuvchiga tegishli bo‘ladi, ushbu foydalanuvchini autentifikatsiya qilish uchun bir martalik parollarni generatsiya qiladi (10-rasm).

OTP tokenlar bir martalik parollarni generatsiya qilish uchun kriptografik algoritmlardan foydalaniladi:

- simmetrik kriptografiya – foydalanuvchi va server autentifikatsiyada bitta o‘sha maxfiy kalitdan foydalanadi;
- assimetrik kriptografiya – ushbu holatda qurilmada maxfiy kalit, serverva esa ochiq kalit ishlatiladi.

OTP larni generatsiya qilishda bir qancha dasturlar yoki qurilmalardan foydalanish mumkin, masalan shaxsiy raqamli qurilmalardan, mobil telefonlardan, yanada xavfsiz bo‘lgan bo‘lgan smart-kartalar ajratilgan apparat tokenlar barcha OTP genratorlari ichida ikki tomonlama autentifikatsiyani ta’minlovchi qurilmalar hisoblanadi. Quyida OTP ni yaratish uchun zarur bo‘lgan uchta qadam keltirilgan (1-rasm): ishlatiladagan qurilmalar hamda autentifikatsiyalash serveri bilan birgalikda ishlatiladigan maxfiy kalitga asoslangan shifrlash algoritmi, sinxron OTP uchun vaqt, assinxron OTP uchun so‘rov kabi bir qancha tashqi ma’lumotlar to‘plami hamda OTP o‘lchamini (xonalar soni 6-8 gacha bo‘lishini ta’minlash uchun) sozlaydigan formatlash qadami.



1-rasm. OTP ni generatsiyalash

OTP algoritmlari maxfiy kalit va qurilma hamda serverlar bilan birgalikda ishlaydigan xisoblagichlarga asoslangan holda ishlab, SHA-1 va HMAC ga o‘xshagan standart algortmlardan foydalanadi. OTP ochiq kalitli infratuzilmalar oldidda juda katta afzalliklarga ega, chunki u shaxsiy kompyuterlar uchun dasturiy ta’minot, drayverlar hamda smart-card reader larni ishlatishni talab qilmaydi [8].

Autentifikatsiyalash tizimi ishlash prinsipi - xavfsizlik autentifikatsiyalash tizimlari talablarining muhim bo‘lgan elementlaridan biri. Foydalanuvchilarning mobil qurilmalari yordamida generatsiya qilingan ma’lumot orqali serverdan avtorizatsiyadan o‘tgan holdagina faqat qonuniy foydalanuvchilar xizmatlarni taqdim etishi asosida xavfsiz jarayon orqali identifikatsiyalash. Bundan tashqari, qulaylik xavfsizlik singari juda muhimdir, chunki autentifikatsiya tizimning noqulayligi tizimdan foydalanishdan voz kechishga olib keladi. Shuning uchun autentifikatsiyalash tizimi qulaylik bilan maksimal xavfsizlikni ta’minlashi kerak bo‘ladi [9].

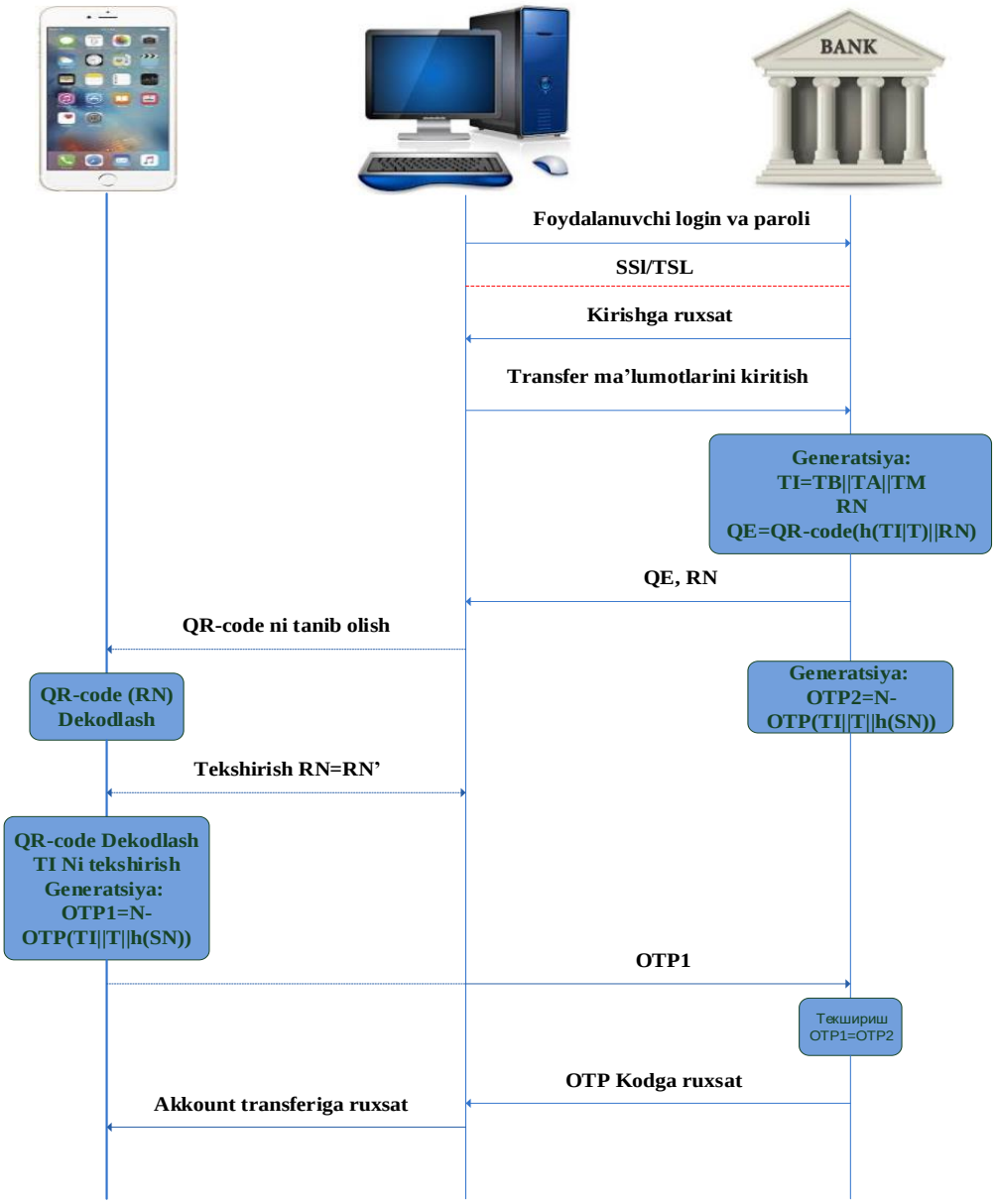
Shu sababli ushbu bitiruv ishida tavsiya etilayotgan yondashuv, bank xavfsizlik kartasi o‘rniga QR-code bilan mobile-OTP ni ishlatish muhim hisoblanadi. Bank foydalanuvchi kiritgan transfer ma’lumotlari orqali QR-code generatsiya qiladi va foydalanuvchi ushbu kodni o‘zining mobil qurilmasi yordamida o‘qib olingan ma’lumot bilan birga qurilma serial nomerining xesh qiymati orqali OTP generatsiya qiladi. Nihoyat foydalanuvchi tomonidan yaratilgan OTP ni yekranga kiritish orqali jarayon tugallanadi. Taklif qilinayotgan sxemada foydalanuvchi kompyuteri bilan xizmat ko‘rsatish serveri o‘rtasida xavfsiz aloqa kanalini o‘rnatamiz.

Taklif qilinayotgan sxemada quyidagi vazifalar bajariladi:

- foydalanuvchi bilan bank serveri foydalanuvchi mobil qurilmasi serial nomerininig xeshini xavfsiz jarayon orqali almashishadi;
- foydalanuvchi QR-code ni o‘zining mobil qurilmasi yordamida tanib olib, kodni ochishi mumkin;
- foydalanuvchi bilan bank serveri o‘rtasida xavfsiz aloqa kanali SSL/TSL mavjudligi taklif qilinadi;
- foydalanuvchi bank serveri tomonidan berilgan OTP-generatorini (algoritmini) yuklab oladi;

generatsiya qilinadigan OTP algoritmi, foydalanuvchi bilan bank serveri o‘rtasida Time-Event usuli orqali sinxronlashtiradi.

Quyida taklif etilayotgan tizim arxitekturasi keltirilgan (2-rasm).



2-rasm. Autentifikatsiyalash sxemasi

Foydalanuvchi o‘zinig login va paroli orqali tizimga kirishni amalga oshiradi, so‘ngra tranzaksiyani amalga oshirish uchun transfer ma’lumotlarini serverga yuboradi.

Transfer ma’lumotlari (TI)=TB||TA||TM

TB=bank kodi.

TA=trantfer akkaunti.

TM= transfer mablag‘i.

Server foydalanuvchi yuborgan transfer ma’lumotlaridan, talab qilinadigan transfer vaqtidan T foydalangan holda ularning xesh qiymatini olib, tasodifiy qiymat RN’ larning QR-code ga aylantiradi va foydalanuvchiga yuboradi.

Foydalanuvchi olingan QR-code ni o‘zining mobil qurilmasi orqali o‘qib olib, ma’lumotni ikki qismga ajrataida. Birinchi QR-code dan o‘qib olgan tasodifiy son RN

ni server yuborgan tasodifiy son RN' bilan solishtiradi. Agar tasodifiy son to‘g‘riligi aniqlansa foydalanuvchi keyingi qadamga o‘tadi. Keyingi qadamda o‘qib olingan transfer ma'lumotlarini tekshirishda va ularning ham xaqiyqiyligini teshirib, so‘ngra mobil qurilmadan foydalangan holda OTP bir martalik parollarni generatsiya qilishga o‘tadi. Agar ma'lumotlar bir biriga mos kelmasa transfer to‘xtatiladi.

Foydalanuvchi OTP ni generatsiya qilish uchun, mobil qurilma orqali transfer ma'lumot bilan vaqt qiymatinidan hamda mobil qurilma serial nomeridan foydalangan holda bir martalik parol generatsiya qiladi. Shu vaqtning o‘zida server ham parallel ravishda ushbu qiymatlardan foydalangan holda bir martalik parol generatsiya qiladi.

Foydalanuvchi mobil qurilma yordamida generatsiya qilingan bir OTP1 ni tizimga yuboradi va tizim serverdagi generatsiya qilingan OTP2 bilan solishtiradi. Agar tekshiruv muvofaqqiyatli amalga foydalanuvchiga transferni amalga oshirishga ruxsat beradi.

Xavfsizlik nuqtai nazardan foydalanuvchi bilan bakn o‘rtasida aloqa kanali SSL/TSL xavfsiz aloqa o‘rnatilgan bo‘ladi. G‘arazli maqsaddagi foydalanuvchilarning ushbu kanalda kontentlarni o‘qib olishga yo‘l qo‘yilmaydi. Shu bilan birgalikda foydalanuvchilarning mobil qurilmalarining serial nomerlaridan foydalanilgani xavfsizlikni oshirishga xizmat qiladi. Ushbu taklif qilinayotgan autentifikatsiyalash tizimida foydalanuchilar Phishing xujumlardan, tasodifiy sonni identifikatsiya qilish orqali himoyalangan bo‘ladi. Foydalanuvchining xaqiyqiyligi tasdiqlangandan so‘ng tranzaksiyani amalga oshirish mumkin bo‘ladi.

XULOSA

QR kodli Mobile-OTP yordamida Onlayn-Bank tizimining autentifikatsiyasi foydalanuvchilarning bank ma'lumotlarini himoya qilishning xavfsiz va qulay usuli hisoblanadi. QR kodlari foydalanuvchilarga bir martalik parollarni tez va oson olish imkonini beradi, ularni o‘g‘irlab bo‘lmaydigan yoki buzg‘unchilar tomonidan tutib olinmaydi. Bu bank hisobiga ruxsatsiz kirish xavfini kamaytiradi va onlayn banking xavfsizlik darajasini oshiradi. QR-kod bilan Mobile-OTP-dan foydalanish bir nechta parollarni eslab qolish zaruratini kamaytirish va foydalanuvchi tajribasini yaxshilash orqali foydalanuvchilarning hayotini osonlashtiradi. Ushbu autentifikatsiya usuli Yevropa Ittifoqidagi To‘lov xizmatlari direktivasi (PSD2) kabi tartibga soluvchi organlarga ham mos keladi, shuning uchun banklar o‘zlarining qonuniy muvofiqligiga ishonch hosil qilishlari mumkin. Ushbu usuldan foydalanadigan banklar o‘z mijozlariga onlayn-bankda yuqori darajadagi xavfsizlikni ta'minlab, bank xizmatlaridan foydalanish jarayonini foydalanuvchilar uchun yanada qulay va xavfsiz qilishga yordam beradi.

ADABIYOTLAR RO‘YXATI

1. Wang, Y., Zhang, Y., & Chen, L. (2011). Two-factor authentication for online banking using mobile phones. Journal of Network and Computer Applications, 34(1), 108-118.
2. Hossain, M. A., & Shamsuddin, S. M. (2016). A secure mobile-based authentication for online banking using QR code. Journal of Information Security and Applications, 26, 26-38.
3. Liu, H., Ma, Y., & Huang, L. (2020). A Survey on Security and Privacy Issues in Mobile Banking Applications. Future Internet, 12(4), 63. https://doi.org/10.3390/fi12040063.
4. Al-Saqaf, W., & Awad, A. (2019). Mobile Banking Security: A Comparative Study of Authentication Methods. Journal of Information Privacy and Security, 15(3), 115-131. https://doi.org/10.1080/15536548.2019.1676005.
5. European Banking Authority. (2019). Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2).
6. Federal Financial Institutions Examination Council. (2016). Authentication and Access to Financial Institution Services and Systems.
7. National Institute of Standards and Technology. (2017). Digital Identity Guidelines: Authentication and Lifecycle Management. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.
8. Chen, Y., & Gong, Y. (2021). A survey of online banking authentication: Challenges and solutions. Journal of Network and Computer Applications, 178, 102978. https://doi.org/10.1016/j.jnca.2021.102978.
9. Kshetri, N., & Voas, J. (2019). Blockchain-enabled secure online voting system. Journal of Organizational Computing and Electronic Commerce, 29(4), 279-296. https://doi.org/10.1080/10919392.2019.1613412.
10. Zawoad, S., Hasan, R., & Hasan, M. (2018). A comprehensive survey on security and privacy issues of mobile banking and solutions to address them. Journal of Network and Computer Applications, 106, 1-26. https://doi.org/10.1016/j.jnca.2017.12.005.
11. National Institute of Standards and Technology. (2017). Digital Identity Guidelines: Enrollment and Identity Proofing. https://doi.org/10.6028/NIST.SP.800-63-2.

12. International Association of Privacy Professionals. (2019). GDPR Compliance and Data Protection for Financial Institutions. https://iapp.org/media/pdf/resource_center/IAPP-[GDPR](poe://www.poe.com/_api/key_phrase?phrase=GDPR&prompt=Tell%20me%20more%20about%20GDPR.)-Compliance-and-Data-Protection-for-Financial-Institutions.pdf.

13. Zhang, Y., & Chen, L. (2010). A survey of two-factor authentication schemes in wireless networks. Computer Communications, 33(9), 1071-1081. https://doi.org/10.1016/j.comcom.2010.02.001

14. Gao, J., Wang, X., & Li, H. (2021). A novel anonymous two-factor authentication scheme for online banking based on biometric and password. Multimedia Tools and Applications, 80(18), 27501-27519. https://doi.org/10.1007/s11042-021-10830-8.

15. European Central Bank. (2018). Cyber resilience oversight expectations for financial market infrastructures. https://www.ecb.europa.eu/paym/cyberresilience/html/index.en.html

16. American Bankers Association. (2018). The State of Bank and Credit Union Digital Marketing. https://www.aba.com/-/media/documents/2018-digital-marketing-report.pdf