



eSIM INTEGRATSIYASI SAMARADORLIGINI OSHIRISH UCHUN PROTOKOLLAR VA METODLAR TAQQOSLANISHI

Alishev Sh.A.

Sambhram universiteti Axborot texnologiyalari muhandisligi kafedra mudiri

Quvandiqov S.

Sambhram universiteti Axborot texnologiyalari fanlari magistranti

Annotatsiya: Ushbu maqolada eSIM (embedded SIM) texnologiyasining mohiyati va uning mobil aloqa sohasida an'anaviy SIM-kartalarni almashtiruvchi innovatsion yechim sifatidagi ahamiyati yoritilgan. Tadqiqotda eSIM integratsiyasida qo'llaniladigan asosiy protokollar — RSP, SGP va ES oilalari hamda Push, Pull va Hybrid integratsiya modellari tahlil qilinadi. Har bir yondashuvning afzalliklari va cheklovlari qiyoslab ko'rsatiladi, shuningdek samaradorlikni oshirish strategiyalari (keshirlash, parallel yuklash, xavfsizlikni optimallashtirish, API integratsiyasi) ishlab chiqilgan. Amaliy jihatdan to'g'ri protokolni tanlashda maqsadli bozor, qurilma turlari, xavfsizlik talablari va mavjud infratuzilmaning roli ochib berilgan. Bundan tashqari, eSIM ekotizimida doimiy monitoring, optimallashtirish va xavfsizlikni ta'minlashning muhimligi asoslab berilgan. Kelajak istiqbollari sifatida eSIMning 5G, IoT, AI/ML va Blockchain texnologiyalari bilan integratsiyasi muhokama qilingan. Tadqiqot natijalari eSIM texnologiyasini joriy etish va rivojlantirishda samarali strategiya ishlab chiqishga xizmat qiladi.

Kalit: so'zlar: eSIM, embedded SIM, RSP protokoli, SGP standartlari, ES interfeyslari, SM-DP+, SM-SR, eUICC, LPA, Push modeli, Pull modeli, Hybrid yondashuv, IoT, 5G, AI/ML, Blockchain, xavfsizlik, masofaviy SIM boshqaruvi, integratsiya samaradorligi, mobil aloqa texnologiyalari.

Kirish

eSIM (embedded SIM) texnologiyasi an'anaviy fizik SIM-kartalarni almashtiruvchi zamonaviy yechim sifatida mobil aloqa sohasida inqilobiy o'zgarishlarni keltirib chiqarmoqda. Ushbu maqolada eSIM integratsiyasini samarali amalga oshirish uchun qo'llaniladigan asosiy protokollar va metodlar tahlil qilinadi hamda ularning afzalliklari va kamchiliklari taqqoslanadi.

eSIM texnologiyasining asoslari

eSIM - bu qurilmaga doimiy ravishda o'rnatilgan qayta dasturlanadigan SIM chip bo'lib, u masofadan turib mobil operator profillarini yuklab olish va boshqarish imkonini beradi. An'anaviy SIM-kartalardan farqli o'laroq, eSIM foydalanuvchilarga fizik kartani almashtirishsiz operatorlarni o'zgartirish imkoniyatini yaratadi.

eSIM (embedded SIM) — bu an'anaviy plastik SIM karta o'rniga qurilmaga integratsiyalangan raqamli SIM bo'lib, bir qancha muhim afzalliklarni taqdim etadi: birinchidan, fizik SIM joyi va uyasi olib tashlangani bois qurilma dizaynida joy va og'irlik



tejaydi, bu kichikroq, suv-va changga chidamli va estetik jihatdan osonroq korpuslarni yaratishga imkon beradi; ikkinchidan, eSIM bir nechta operator profillarini saqlay oladi va foydalanuvchi yoki tizim ularni tezda almashtirishi yoki faollashtirishi mumkin — bu sayohat, dual-SIM talablar yoki operatorlararo sinovlar uchun juda qulay; uchinchidan, eSIM profillarini masofadan (OTA) boshqarish va sozlash mumkinligi tufayli qurilmalarni ommaviy ishlab chiqish va IoT loyihalarida SIMlarni jismoniy almashmay turib butun parkni qayta konfiguratsiya qilish, yangilash va qayta yo'naltirish soddalashadi; to'rtinchidan, plastik kartalar va ularning qadoqlanishini kamaytirishi atrof-muhitga ijobiy ta'sir ko'rsatadi — chiqindilar va transport xarajatlari kamayadi; va nihoyat, xavfsizlik jihatidan eSIMlar maxsus xavfsiz elementlarda (secure element) saqlanadi, profiling shifrlash, operator bilan kuchli autentifikatsiya va sertifikatlash orqali yuqori darajadagi kriptografik himoya ta'minlaydi, bu esa sim-o'g'irlash va noxush manipulyatsiyalarga nisbatan qo'shimcha himoya beradi — shuning uchun eSIMlar ayniqsa smart soatlar, IoT qurilmalari, avtomobil va korporativ ilovalarda keng qo'llanilmoqda.

Remote SIM Provisioning (RSP) protokoli — bu GSMA tomonidan ishlab chiqilgan va eSIM profillarini masofadan boshqarish, ya'ni ulardan foydalanish, yangilash yoki o'chirish imkonini beruvchi global standartdir. U ikkita asosiy arxitekturaga ega bo'lib, ulardan biri M2M (Machine-to-Machine) bo'lib, asosan IoT qurilmalari, avtomobillar va aqlli sensorlarda qo'llaniladi. Ushbu arxitekturada uchta muhim komponent mavjud: SM-SR (Subscription Manager – Secure Routing) serveri — eSIM bilan xavfsiz aloqa o'rnatib, profilni yetkazib berish, faollashtirish va o'chirish jarayonini boshqaradi; SM-DP (Subscription Manager – Data Preparation) serveri — mobil operator profillarini tayyorlab, shifrlangan ko'rinishda SM-SR ga yuboradi; eUICC (embedded Universal Integrated Circuit Card) esa qurilmaga o'rnatilgan chip bo'lib, eSIM profillarini saqlaydi hamda ularni faollashtirish va boshqarishni ta'minlaydi. Shu tarzda RSP protokoli foydalanuvchi aralashuvisiz qurilmalarni masofadan turib boshqarish imkoniyatini beradi.

Consumer arxitekturasi esa asosan smartfonlar, planshetlar va boshqa iste'molchi qurilmalarida qo'llaniladi va unda SM-DP+ (Subscription Manager Data Preparation +) serveri asosiy rol o'ynaydi. Bu server SM-DP va SM-SR funksiyalarini birlashtirgan bo'lib, eSIM profillarini yaratish, saqlash va qurilmaga yetkazib berishni boshqaradi. Qurilma ichida LPA (Local Profile Assistant) moduli mavjud bo'lib, u foydalanuvchi ilovasi orqali eSIM profillarini yuklab olish, faollashtirish yoki o'chirish imkonini beradi. Shuningdek, eUICC (embedded Universal Integrated Circuit Card) eSIM chipining o'zini anglatadi va unda profillar xavfsiz tarzda saqlanadi. Shu tarzda consumer arxitekturasi foydalanuvchilarga operator profillarini qulay, tezkor va xavfsiz boshqarish imkoniyatini yaratadi. SGP protokollari seriyasi – bu GSMA tomonidan ishlab chiqilgan spetsifikatsiyalar to'plami bo'lib, eSIM ekotizimini turli qurilmalar va platformalar uchun yagona standart asosida ishlashini ta'minlaydi. Masalan, SGP.21 – Consumer Solution arxitekturasini belgilaydi va foydalanuvchi qurilmalarida (smartfon, planshet va boshqalar) eSIM qanday ishlashini tushuntiradi. SGP.22 esa shu arxitektura uchun texnik





spetsifikatsiyalarni taqdim etib, operatorlar, qurilma ishlab chiqaruvchilar va dasturiy ta'minot ishlab chiquvchilar uchun aniq ko'rsatmalar beradi. IoT qurilmalar uchun esa alohida standartlar ishlab chiqilgan: SGP.31 – IoT uchun yangi arxitekturani belgilaydi, ya'ni turli sanoat qurilmalari, sensorlar va aqlli texnologiyalarni eSIM orqali samarali ulash va boshqarish imkonini yaratadi. SGP.32 esa IoT arxitekturasini uchun texnik spetsifikatsiyalarni ishlab chiqib, xavfsizlik, profil boshqaruvi va qurilmalararo moslikni ta'minlashga qaratilgan. Shu bilan, SGP seriyasi eSIM texnologiyasining iste'molchi qurilmalaridan tortib IoT tizimlarigacha global miqyosda barqaror va standart asosda ishlashini kafolatlaydi.

ES protokollari (Embedded SIM protokollari) – bu eSIM ekotizimida turli komponentlar o'rtasida o'zaro aloqa va ma'lumot almashinuvini ta'minlovchi interfeyslar majmuasidir. Ularning asosiy vazifasi eSIM profilini yaratish, yetkazish, o'rnatish va boshqarish jarayonini standartlashtirishdir. Masalan, ES2+ – bu SM-DP+ (Subscription Manager – Data Preparation) va mobil Operator o'rtasidagi interfeys bo'lib, unda operator profillari tayyorlanadi va SM-DP+ ga yuboriladi. ES9+ – bu SM-DP+ va LPA (Local Profile Assistant) o'rtasidagi interfeys bo'lib, foydalanuvchi qurilmasiga profilni yuklab olish va o'rnatishni ta'minlaydi. ES10 esa LPA va eUICC (embedded UICC) o'rtasidagi interfeys bo'lib, qurilma ichidagi eSIM chipiga profilni o'rnatish, faollashtirish va boshqarishni amalga oshiradi. Shu tarzda, ES protokollari eSIM ekotizimining barcha bosqichlarida – operator profilini yaratishdan tortib foydalanuvchi qurilmasida to'liq ishlashigacha – uzluksiz aloqani ta'minlaydi.

Push model — eSIM integratsiyasida ishlatiladigan usullardan biri bo'lib, bunda profilni qurilmaga yuklash jarayoni operator tomonidan to'liq boshqariladi, foydalanuvchining ishtiroki esa minimal darajada bo'ladi. Bu metod asosan korporativ muhitlarda qo'llanadi, chunki u markazlashtirilgan boshqaruvni ta'minlaydi va bir vaqtning o'zida ko'plab qurilmalarga profilni avtomatik tarzda yuklash imkonini beradi. Uning afzalliklariga markazlashtirilgan boshqaruv, avtomatlashtirilgan jarayonlar va kuchli xavfsizlik nazorati kiradi. Shu bilan birga, kamchiliklari ham mavjud: foydalanuvchi nazorati cheklanganligi, profilni qo'lda tanlash imkoniyatining yo'qligi va moslashuvchanlikning pastligi. Shu sababli, Push model asosan korporativ tashkilotlar, IoT tarmoqlari va xavfsizlik darajasi yuqori bo'lishi talab qilinadigan tizimlarda samarali hisoblanadi.

Pull model — bu eSIM integratsiyasi metodlaridan biri bo'lib, unda profilni yuklash jarayonini foydalanuvchi o'zi boshqaradi. Odatda foydalanuvchi QR kodni skanerlash yoki aktivatsiya kodini kiritish orqali mobil operator profilini qurilmaga o'rnatadi. Ushbu yondashuv asosan iste'molchilar uchun mo'ljallangan, chunki u qulay, tez va oddiy jarayonni ta'minlaydi. Afzalliklari shundaki, foydalanuvchi profilni tanlash va faollashtirish ustidan to'liq nazoratga ega bo'ladi, jarayon oddiy va intuitiv ko'rinishda bo'ladi hamda tez o'rnatish imkonini beradi. Shu bilan birga, kamchiliklari ham mavjud: foydalanuvchi tomonidan kodni noto'g'ri kiritish yoki QR kodni noto'g'ri skanerlash kabi xatoliklar



yuzaga kelishi mumkin, shuningdek, bu modelda avtomatlashtirish darajasi past bo'ladi. Shuning uchun Pull model ko'proq shaxsiy iste'molchilar uchun samarali bo'lsa, korporativ va IoT tizimlarida esa Push model afzalroq hisoblanadi.

Hybrid model — bu eSIM integratsiyasi jarayonida Push va Pull modellarning kombinatsiyasi bo'lib, foydalanuvchiga ham mustaqil boshqaruv imkonini beradi, ham operator tomonidan markazlashtirilgan boshqaruvni qo'llab-quvvatlaydi. Ushbu yondashuv kontekstga qarab moslashuvchanlikni ta'minlaydi: masalan, korporativ muhitda Push modeli asosiy bo'lsa, iste'molchi qurilmalarida Pull modeli ishlatilishi mumkin. Afzalliklari shundaki, u maksimal moslashuvchanlikni taqdim etadi, turli xil foydalanish holatlarini qamrab oladi va foydalanuvchiga qulay hamda optimallashtirilgan tajribani yaratadi. Biroq, kamchiliklari ham bor: bunday tizimni ishlab chiqish va joriy qilish murakkabroq bo'ladi hamda yuqori darajadagi rivojlanish va texnik xizmat ko'rsatish xarajatlarini talab qiladi.

eSIM integratsiyasida samaradorlikni oshirish strategiyalari bir necha yo'nalishda amalga oshiriladi. Birinchi navbatda, keshirlash va ma'lumotlarni optimallashtirish orqali profil yuklanish jarayonini tezlashtirish mumkin: tez-tez ishlatiladigan ma'lumotlarni lokal keshda saqlash, profillarni minimal hajmda tayyorlash va ma'lumotlarni siqish algoritmlaridan foydalanish yuklash vaqtini sezilarli qisqartiradi. Ikkinchidan, parallel yuklash strategiyasi bir nechta profilni bir vaqtning o'zida yuklash imkonini berib, vaqtni tejash, resurslardan samarali foydalanish va yuqori o'tkazish qobiliyatidan maksimal darajada foydalanish imkonini beradi. Uchinchidan, xavfsizlik optimallashtirish orqali samaradorlik pasaymasdan yuqori darajadagi himoya ta'minlanadi: zamonaviy shifrlash algoritmlaridan foydalanish, sertifikatlarni avtomatlashtirilgan tarzda boshqarish va xavfsizlik tekshiruvlarini samarali tashkil qilish muhimdir. Nihoyat, API integratsiyasi (RESTful API va webhook'lar) real vaqt rejimida sinxronizatsiya qilish, avtomatik xabarnomalar yuborish va turli tizimlar o'rtasida uzluksiz integratsiya yaratish imkonini beradi. Shu tarzda, ushbu strategiyalar kombinatsiyasi eSIM ekotizimining tezkor, xavfsiz va barqaror ishlashini ta'minlaydi. (Jadval -1)

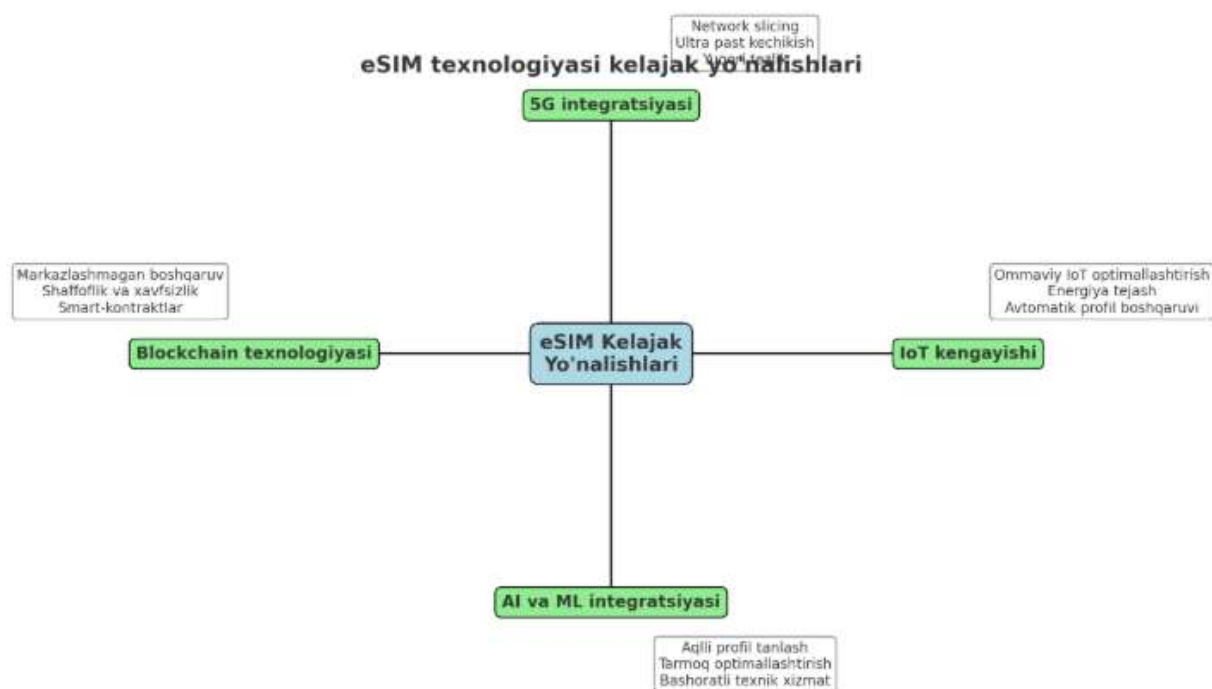
Strategiya	Asosiy g'oya	Afzalliklari	Kamchiliklari
Keshirlash va ma'lumotlarni optimallashtirish	Profil hajmini kichraytirish, tez-tez ishlatiladigan ma'lumotlarni keshda saqlash, siqish	Yuklash tezlashadi, kam resurs sarfi, tarmoqdan mustaqillik	Kesh sinxronlashda muammolar, qo'shimcha xotira talab qiladi
Parallel yuklash	Bir nechta profilni bir vaqtning o'zida yuklash	Vaqtni tejaydi, resurslardan samarali foydalanadi, throughput oshadi	Murakkab boshqaruv, ko'p tarmoqli jarayonlarda xatolik xavfi
Xavfsizlik optimallashtirish	Shifrlashni samarali qilish, sertifikatlarni	Xavfsizlik va tezlik birga ta'minlanadi	Kuchli algoritmlar ko'proq hisoblash

	boshqarish, tekshiruvlarni yengillashtirish		quvvatini talab qilishi mumkin
API integratsiyasi	RESTful API va webhook'lar orqali real vaqtda ishlash	Avtomatlashtirish, tezkor sinxronizatsiya, tizimlararo moslik	API xavfsizligi muammosi, qo'shimcha dasturlash xarajatlari

Buning uchun to'g'ri protokolni tanlashda maqsadli bozor (iste'molchi vs korporativ/M2M), qurilma turlari (smartfon, wearables, IoT sensorlar yoki avtomobil), talab qilinadigan xavfsizlik darajasi (end-to-end shifrlash, PKI/HSM asosidagi kalitlar, sertifikatlar va audit) hamda mavjud infratuzilmani (backend, OTA kanallari, DB va kesh tizimlari, CI/CD) birgalikda qiymatlang — masalan, iste'molchi qurilmalar uchun SGP.21/22 va SM-DP+ + LPA qulay, M2M/IoT uchun esa SGP.31/32 va markazlashtirilgan SM-SR/SM-DP arxitekturasini afzaldir; test muhitini yaratishda esa alohida staging klasterini tashkil qiling va unda SM-DP+, SM-SR va eUICC/LPA emulyatorlarini ishga tushirib turli stsenariylarni sinab chiqing: normal provisioning, parallel/koncurrent provisioning (thundering herd), past tarmoqli o'tkazuvchanlik va yuqori kechikish sharoitlari, profil almashtirish/rollback, kalit/sertifikat yangilanishi va kompromat holatlari; yuklash testlari (throughput, stress, soak) uchun JMeter yoki Locust kabi vositalardan foydalanib p95/p99 latentsiyalarni, provisioning per second va xatolik stavkalarini o'lchang; monitoring va tahlil qismida esa aniq KPIlar belgilang — provisioning muvaffaqiyat foizi, o'rtacha provisioning vaqti, xato (failure) darajasi, qayta urinuvlar soni, CPU/RAM va disk I/O, DB replikasiya lag, kesh hit ratio va audit log hajmi — bu metrikalarni Prometheus/Grafana orqali vizualizatsiya qilib alertlar o'rnatish, log va tracing (ELK/Tempo) bilan root-cause tahlilini osonlashtiring; operatsion jihatdan SLO/SLAs belgilang, canary va staged rollout amaliyotini joriy eting, zaxira/recovery rejalarini hamda muntazam xavfsizlik skanerlari, penetration testlar va kalitlarni HSMda saqlash kabi amaliyotlarni qo'llang — shu tarzda protokol tanlash, puxta testlash va doimiy monitoring orqali eSIM integratsiyasi xavfsiz, barqaror va samarali bo'ladi.

Kelajak istiqbollari nuqtai nazaridan eSIM texnologiyasi tez sur'atlar bilan rivojlanmoqda va bir nechta muhim yo'nalishlarni o'z ichiga oladi. Birinchidan, 5G integratsiyasi orqali eSIM network slicing imkoniyatlarini qo'llab-quvvatlab, ultra past kechikish va yuqori tezlikni ta'minlashi kutilmoqda, bu esa real vaqtda ishlovchi ilovalar va yangi avlod xizmatlari uchun asos bo'ladi. Ikkinchidan, IoT kengayishi jarayonida eSIM milliardlab IoT qurilmalarini ulash uchun optimallashtiriladi, energiya tejash mexanizmlari ishlab chiqiladi va avtomatik profil boshqaruvi joriy etiladi, bu esa masshtablanishni yengillashtiradi. Uchinchidan, AI va ML integratsiyasi yordamida eSIM tizimlari aqlli profil tanlashni amalga oshiradi, tarmoq yuklamasini dinamik optimallashtiradi va

bashoratli texnik xizmat ko'rsatishni ta'minlaydi. Nihoyat, Blockchain texnologiyasi markazlashmagan profil boshqaruvi, shaffoflik va xavfsizlikni oshirish bilan birga smart-kontraktlar orqali avtomatlashtirilgan jarayonlarni yo'lga qo'yadi. Shu tariqa, eSIM kelajakda ko'proq moslashuvchan, xavfsiz va aqlli tizim sifatida mobil aloqa va IoT ekotizimining markazida bo'ladi. (Rasm-1)



Xulosa

eSIM integratsiyasini muvaffaqiyatli amalga oshirish uchun avvalo biznes talablarini (iste'molchi vs korporativ, qurilma turlari, xavfsizlik va skalabilite talablari) aniqlab, shunga mos protokolni tanlashingiz zarur — RSP/SGP oilasi iste'molchi va M2M ehtiyojlariga mo'ljallangan va SM-DP+/SM-SR komponentlari qanday ishlashini loyihaga moslashtirish kerak; amaliyotda esa Push va Pull imkoniyatlarini birlashtirgan hybrid yondashuv ko'plab holatlar uchun optimal yechim bo'lib, u markazlashtirilgan boshqaruv hamda foydalanuvchi nazoratini birlashtiradi; xavfsizlik va samaradorlik o'rtasida muvozanat saqlash uchun PKI/HSM asosida kalitlarga ega bo'lish, zamonaviy shifrlash va sertifikat boshqaruvi, qisman tekshiruvlarda tezlikni oshirish uchun siqish va keshirlashni qo'llash, shuningdek parallel provisioning imkoniyatlarini joriy etish foydali; tizim ishga tushgach, doimiy monitoring va optimallashtirish — provisioning muvaffaqiyat ko'rsatkichi, p95/p99 latentsiyalar, kesh hit-rate, log/trace yig'ish va alertlar orqali — muntazam o'lchanib, canary/staged rollout va rollback rejalariga asoslangan yangilash siyosati orqali amalga oshirilsin; va nihoyat, 5G, mass-IoT, AI/ML va blokcheyn kabi kelajak texnologiyalariga moslashuvchan arxitektura (modullilik, API-first dizayn, indexlangan va asinxron indexing pipeline) tayyorlab qo'yilsin — shu tarzda sizning eSIM strategiyangiz nafaqat xavfsiz va samarali bo'ladi, balki bozor sharoitida raqobatbardosh ustunlik ham beradi.



Foydalanilgan adabiyotlar ro'yxati:

- [1] Yuan, H., Baloian, A., Janak, J., & Schulzrinne, H. (2024). *eSIM Technology in IoT Architecture*. arXiv preprint arXiv:2401.04302.
- [2] Ahmed, A. S., Peltonen, A., Sethi, M., & Aura, T. (2022). *Security Analysis of the Consumer Remote SIM Provisioning Protocol*. arXiv preprint arXiv:2211.15323.
- [3] Barros, S., et al. (2025). *Trusted Identities for AI Agents: Leveraging Telco-Hosted eSIM Infrastructure*. arXiv preprint arXiv:2504.16108.
- [4] Ebadi, S., Moolman, Z., Keller, E., et al. (2025). *Decoupling the Device and Identity in Cellular Networks with vSIM*. arXiv preprint arXiv:2505.15827.
- [5] Zhang, Y., et al. (2023). *eSIM and blockchain integrated secure zero-touch provisioning for IoT-SAFE protocol*. *Computer Communications*, 205, 90–102.
- [6] GSMA. (2023). *SGP.32 eSIM for IoT: Technical Specification*. GSMA Whitepaper.
- [7] Eseye. (2023). *SGP.32 eSIM Readiness – A New Frontier for IoT Strategies*. Retrieved from <https://www.eseye.com>.
- [8] UzDaily. (2022). *Mobiuz launches eSIM technology in Uzbekistan*. Retrieved from <https://www.uzdaily.uz>.