KRIPTOTURTO SAUGOJIMAS IR ADMINISTRAVIMAS

Šioje UAB Decentralized (toliau – Bendrovė) Kriptoturto saugojimo politikoje, parengtoje pagal Europos Sąjungos Kriptoturto rinkų reglamentą ir Skaitmeninės veiklos atsparumo aktą (DORA), nustatomos procedūros ir kontrolės priemonės, skirtos Klientų kriptoturto saugiam laikymui ir valdymui. Šios politikos tikslas – sumažinti turto praradimo riziką, užtikrinti tikslų ir išsamų apskaitos tvarkymą bei užtikrinti skaidrumą dėl saugojimo sąlygų ir su tuo susijusių rizikų. Joje taip pat apibrėžiama, kaip Bendrovė saugo Klientų turtą taikydama atskyrimą, prieigos kontrolės priemones, kriptografinių raktų gyvavimo ciklo valdymą ir veiklos tęstinumo planavimą. Politika reguliariai peržiūrima ir atnaujinama, atsižvelgiant į pasikeitusius reglamentavimo reikalavimus, techninę infrastruktūrą ir vidinę praktiką.

PAGRINDINĖS BENDROVĖS TEIKIAMŲ SAUGOJIMO PASLAUGŲ SUDEDAMOSIOS DALYS

- **Saugumo priemonės.** Techninės ir procedūrinės kontrolės priemonės, tokios kaip daugiaveiksnis tapatumo nustatymas, kriptografinių raktų medžiagos šifravimas, prieigos pagal pareigas ribojimas ir saugi piniginės architektūra, apsaugo Kliento Kriptoturtą.
- **Naudotojo sąsaja.** Saugus ir patogus Klientų portalas suteikia Klientams galimybę peržiūrėti likučius, inicijuoti lėšų išėmimą ir valdyti prieigą prie sąskaitos su realiojo laiko atnaujinimais.
- **Sandorių vykdymas.** Klientų inicijuojami sandoriai yra tikrinami automatinėmis ir rankinėmis priemonėmis, siekiant užtikrinti atitiktį, tikslumą ir saugų pristatymą į blokų grandinę.
- **Atkūrimo paslaugos.** Atkūrimo procesas, apimantis tapatybės patvirtinimą pagal oficialius dokumentus, leidžia Klientams atgauti prieigą prie sąskaitos praradus prisijungimo duomenis.
- **Klientų aptarnavimas.** Pagalba teikiama tiesioginiu pokalbiu darbo valandomis ir el. paštu, o visi užklausimai registruojami Bendrovės klientų santykių valdymo sistemoje.
- **Saugojimo funkcijos neperduodamos išorės paslaugų teikėjams.** Visi sprendimai dėl saugojimo, privačių kriptografinių raktų valdymo, prieigos kontrolės ir sandorių autorizavimo atliekami Bendrovės viduje, jos darbuotojų. Bendrovė gali pasitelkti techninės infrastruktūros teikėją (toliau – Techninis paslaugų teikėjas) Šaltųjų ir Giliųjų šaltųjų piniginių valdymui, tačiau Techninis paslaugų teikėjas nelaiko, neturi prieigos ir nekontroliuoja jokių privačių kriptografinių raktų, o Klientų Kriptoturto saugojimas visada lieka tik Bendrovės atsakomybe.

SAUGOJIMO SPRENDIMAI

Bendrovė teikia Kriptoturto saugojimo paslaugas kaip integruotą savo veiklos pasiūlymų dalį. Saugojimas yra būtinas kriptovaliutų mokėjimams, konvertavimui tarp lėšų ir kriptoturto bei kriptoturto išmokėjimams Klientų vardu užtikrinti. Klientų kriptoturtas laikomas atskirosiose piniginėse, kurios yra atskirtos nuo bendrovės turto ir yra visiškai atsekamos bendrovės techninėse bei apskaitos sistemose. Nors atskirosiose piniginėse kriptoturtas telkiamas bendrai, kiekvieno Kliento teisės ir nuosavybės teisės yra individualiai apskaitomos bendrovės vidaus registre.

Naudojamos trijų tipų atskirosios piniginės:

- Gilios šaltosios piniginės (angl. Deep Cold Wallets), kuriose didžioji dalis Klientų kriptoturto laikoma neprisijungus prie interneto. Privačių kriptografinių raktų medžiaga padalinta tarp kelių nepriklausomų aplinkų taip, kad jokia atskira aplinka, įrenginys ar asmuo niekada nelaiko viso privataus rakto, o raktų medžiaga visą savo gyvavimo ciklą yra šifruojama. Prieiga suteikiama tik paskirtiems vyresniesiems vadovams, o sandoriai patvirtinami pagal

kvorumo principą platformos lygmeniu užtikrinant „keturių akių" principą. Sandorį inicijavęs asmuo negali jo patvirtinti pats.

- Šaltosios piniginės (angl. Cold Wallets), kurios taip pat laikomos neprisijungus prie interneto ir naudojamos išmokoms Klientams, tokioms kaip lėšų išėmimai ir grąžinimai. Raktų medžiaga padalinama ir šifruojama panašiai kaip giliosiose šaltosiose piniginėse. Sandoriai formuojami programiškai per bendrovės įgaliotas sistemas ir automatiškai pasirašomi specialiu pasirašymo komponentu bendrovės infrastruktūroje, o paskirties adresai valdomi pagal apibrėžtas kontrolės priemones, užtikrinant pilną audito registravimą.
- Karštosios piniginės (angl. Hot Wallets), kurios yra prijungtos prie interneto ir naudojamos Klientų įnašams priimti bei didelio dažnio automatiniams sandoriams vykdyti per Bendrovės pačios sukurtą kriptoturto valdymo infrastruktūrą (sistemą Argus). Privatūs raktai valdomi naudojant AWS Secrets Manager, talpinamą AWS ES regione, taikant prieigos pagal pareigas valdymą, šifravimą ir automatinius įspėjimus. Karštosiose piniginėse laikomi likučiai sumažinami iki minimumo, periodiškai juos perkeliant į kitas saugojimo vietas.

Bendrovė taiko raktų atsarginio kopijavimo ir atkūrimo procesą, skirtą užtikrinti nenutrūkstamą prieigą prie Klientų kriptoturto įrenginio praradimo, darbuotojo nepasiekiamumo ar infrastruktūros gedimo atveju. Atsarginės kopijos kuriamos specialioje, nuo interneto izoliuotoje (angl. air-gapped) darbo vietoje, šifruoti atsarginių kopijų paketai saugomi atskirai nuo iššifravimo priemonių, o šifruota atsarginių kopijų medžiaga ir jos iššifravimo priemonės laikomos skirtingų įgaliotų darbuotojų. Joks vienas asmuo negali savarankiškai užbaigti viso raktų atkūrimo proceso – jis reikalauja kelių įgaliotų darbuotojų suderintų veiksmų.

Visų tipų piniginės yra prižiūrimos taikant griežtas operacines ir kibernetinio saugumo kontrolės priemones, įskaitant kasdienį suderinimą, raktų gyvavimo ciklo procedūras ir nuolatinę stebėseną. Taikomas saugojimo lėšų telkimas, tačiau individualios Klientų teisės realiuoju laiku registruojamos vidiniame registre. Bendrovės turtas nelaikomas atskirosiose piniginėse, o Klientų kriptoturtas niekada nenaudojamas bendrovės veikloje.

KLIENTŲ POZICIJŲ REGISTRAS

Bendrovė, vadovaudamasi kriptoturto rinkų reglamentu, tvarko saugų realiojo laiko registrą, kuriame fiksuojamas Klientų kriptoturto laikymas. Kiekvienam Klientui registre skiriama atskira dalis, užtikrinanti, kad nuosavybės teisės būtų aiškiai atskirtos, atsekamos ir prieinamos ataskaitų teikimo bei suderinimo tikslais. Visi sandoriai – įnašai, išėmimai ir vidiniai pervedimai – registruojami pagal Klientų nurodymus ir prieš įvykdymą yra kruopščiai tikrinamas tapatumas, užtikrinama atitiktis ir atliekamos patikros procedūros. Įvykdžius sandorį, jis įrašomas su visa informacija, o Klientui išsiunčiamas patvirtinimas. Klientai gali bet kuriuo metu per Klientų portalą peržiūrėti ataskaitas ir kiekvieną mėnesį gauti būklės ataskaitą, kurioje nurodomas turimas kriptoturtas, jo vertė ir likučiai.

REGISTRO TECHNINĖ ARCHITEKTŪRA IR DUOMENŲ SAUGOJIMAS

Bendrovės klientų pozicijų registras sukurtas naudojant PostgreSQL duomenų bazę, valdomą per Amazon Web Services (AWS) Relational Database Service (RDS) platformą, užtikrinančią patikimumą, saugumą ir aukštą pasiekiamumą. Sistema apima dvi duomenų bazes: core-ledger, kurioje registruojamos visos finansinės operacijos pagal dvejybinio įrašo principą, ir core-database, kurioje saugoma susijusi informacija apie operacijas ir klientus. Registras veikia tik pridedant įrašus, todėl neleidžiama keisti ar trinti esamų įrašų. Kiekviena operacija pažymima laiko žyma, turi unikalų identifikatorių ir registruojama nuosekliai. Duomenų vientisumas užtikrinamas taikant dvejybinę apskaitą, privalomus ryšius tarp lentelių ir unikalius indeksus, kurie neleidžia dubliuoti įrašų.

Nuolatinės atsarginės kopijos kuriamos per AWS RDS pagal bendrovės patvirtintas duomenų atsarginių kopijų kūrimo ir atkūrimo procedūras.

KLIENTŲ TURTO ATSKYRIMAS

Bendrovė užtikrina, kad visas Klientų Kriptoturtas būtų laikomas atskirosiose piniginėse, visiškai atskirai nuo bendrovės nuosavo turto. Šis turtas lieka Kliento nuosavybe ir negali būti naudojamas bendrovės veiklai, investicijoms ar įsipareigojimams vykdyti. Vidinė apskaita tiksliai fiksuoja kiekvieno Kliento teises, net ir kai turtas yra telkiamas. Prieiga prie atskirųjų piniginių yra griežtai ribojama tik paskirtiems darbuotojams, o visi sandoriai vykdomi laikantis saugumo protokolų, įskaitant daugiaveiksnį tapatumo nustatymą ir šifravimą. Atsitiktinai gavus Kliento turtą į operacinę piniginę, Bendrovė jį perveda į atitinkamą atskirąją piniginę ne vėliau kaip kitą darbo dieną. Nemokumo atveju Klientų turtas yra apsaugotas nuo bendrovės kreditorių reikalavimų.

RIZIKOS VALDYMAS

Bendrovė aktyviai identifikuoja, stebi ir mažina su kriptoturto saugojimu susijusias rizikas. Tai apima neteisėtą prieigą prie sąskaitos, turto praradimą ar vagystę, techninius gedimus, veiklos klaidas, reguliavimo pažeidimus, rinkos svyravimus ir trečiųjų šalių infrastruktūros riziką, kylančią dėl techninio paslaugų teikėjo naudojimo šaltųjų ir giliųjų šaltųjų piniginių valdymui. Kontrolės priemonės apima šifravimą, daugiaveiksnį tapatumo nustatymą, prieigą pagal pareigas, įsibrovimų aptikimą ir reguliarius auditus. Raktų valdymas vykdomas pagal griežtus gyvavimo ciklo protokolus, su saugiu atsarginių kopijų kūrimu ir kvorumu pagrįstu sandorių patvirtinimu; privačių kriptografinių raktų medžiaga sutvarkyta taip, kad joks atskiras asmuo ar sistema negalėtų savarankiškai pasiekti ar atkurti viso privataus rakto. Techninės rizikos valdomos taikant automatinę stebėseną, pažeidžiamumo skenavimą, kassavaitinį kritinių sistemų automatinį skenavimą ir išbandytas atkūrimo procedūras. Veiklos atsparumą užtikrina pareigų atskyrimas, „keturių akių" principas, privalomi darbuotojų mokymai ir incidentų valdymo procedūros. Trečiųjų šalių infrastruktūros rizika mažinama taikant sutartines apsaugos priemones, periodiškai vertinant techninio paslaugų teikėjo veiklą ir saugumo būklę bei užtikrinant bendrovės gebėjimą perkelti Klientų turtą į savo vidinę atsarginę infrastruktūrą, jeigu techninio paslaugų teikėjo paslaugos sutriktų. Atitiktis reglamentavimui užtikrinama nuolat stebint teisinę aplinką, atnaujinant politikas ir atliekant audito peržiūras pagal kriptoturto rinkų reglamento ir DORA reikalavimus.

KRIPTOTURTUI PRISKIRTŲ TEISIŲ ĮGYVENDINIMAS

Bendrovė neužtikrina su saugomu kriptoturtu susijusių teisių įgyvendinimo, tokių kaip balsavimas, įkeitimas, dalyvavimas valdyme ar protokolo atlygių gavimas. Atsiradus atsiskyrimui (angl. hard fork), pasiskirstymui (angl. airdrop) ar panašiam įvykiui, Klientai neturi teisės į jokią dėl to atsiradusią teisę ar naują turtą, nebent Bendrovė aiškiai nurodo kitaip. Turtas laikomas sutelktose piniginėse, ir joks individualus paskirstymas ar teisė į naudą, kylančią iš tokių įvykių, nėra suteikiami, išskyrus atvejus, kai Bendrovė savo nuožiūra nusprendžia tokį paskirstymą ar palaikymą užtikrinti.

PRIEIGA PRIE SAUGOMO KRIPTOTURTO IR JO GRĄŽINIMAS

Klientai gali bet kuriuo metu saugiai pasiekti ir atsiimti savo kriptoturtą per bendrovės šifruotą Klientų portalą, kuriame taikomas daugiaveiksnis tapatumo nustatymas. Lėšų išėmimo prašymai apdorojami taikant struktūrizuotą ir saugią procedūrą, kuri apima piniginės nuosavybės patvirtinimą, tapatybės nustatymą ir atitikties tikrinimą pagal reglamentavimo reikalavimus. Visa prieigos ir turto grąžinimo veikla yra registruojama, o sąskaitos veiksmai nuolat stebimi siekiant užtikrinti skaidrumą ir sudaryti sąlygas auditui. Jautrioms operacijoms, tokioms kaip sąskaitos saugumo nustatymų keitimas ar naujų

lėšų išėmimo adresų pridėjimas, reikalingas papildomas tapatumo patvirtinimas. Praradę prieigos duomenis, Klientai gali inicijuoti saugų atkūrimo procesą, kurio metu patvirtinama tapatybė pateikiant valstybės išduotą asmens tapatybės dokumentą ir patvirtinami sąskaitos duomenys. Tam tikrose situacijose, tokiose kaip nepalaikomas turtas, sąskaitos uždarymas ar priežiūros institucijų nurodymai, Bendrovė gali grąžinti arba likviduoti kriptoturtą, iš anksto apie tai pranešdama, kai tik įmanoma.

ATSAKOMYBĖ UŽ KRIPTOTURTO PRARADIMĄ

Bendrovė atsako už bet kokį kriptoturto ar prieigos prie jo priemonių praradimą, atsiradusį dėl jos aplaidumo, netinkamo elgesio ar sutartų saugumo protokolų nesilaikymo. Atsakomybė yra ribojama prarasto kriptoturto rinkos verte įvykio metu, nustatyta pagal vidutines kainas pagrindiniuose kriptoturto paslaugų teikėjuose. Bendrovė neatsako už nuostolius, atsiradusius dėl Kliento aplaidumo, duomenų vagystės atakų, su bendrove nesusijusių trečiųjų šalių sistemų saugumo pažeidimų, paskirstytojo registro technologijos veikimo sutrikimų ar force majeure aplinkybių. Atsiradus nuostoliui, bendrovė atliks tyrimą, dokumentuos nustatytas aplinkybes ir informuos nukentėjusius Klientus. Klientai privalo pranešti apie nuostolius per nustatytą laikotarpį. Nustačius bendrovės atsakomybę, bus išmokėta kompensacija. Bendrovė taip pat laikosi pareigos įgyvendinti veiksmingas saugumo kontrolės priemones, teikti informaciją apie rizikas, užtikrinti darbuotojų mokymus ir tiksliai tvarkyti apskaitą, siekiant užkirsti kelią turto praradimui.