Parool, QR-kood ja PIN: kuidas on muutunud veebis sisselogimine?

8 min tagasi - 23.11.2026 Autor: AM

(Sisuturundus)

Veebruari lõpus märkasid paljud Eesti e-teenuste kasutajad sisselogimisaknas uut QR-koodi. Varem tuli sisestada isikukood ja võrrelda kontrollnumbreid. Nüüd saab arvutiekraanil oleva koodi telefoniga skannida ning kinnitada sisselogimise PIN1-ga.

Muudatus jõustus 26. veebruaril 2026, kui Riigi Infosüsteemi Amet võttis kasutusele Smart-ID+ lahenduse. Samal ajal kasutavad paljud muud veebiteenused endiselt paroole, ühekordseid koode või telefonis kuvatavaid kinnitusi.

Mängukonto avamine, sisselogimine ja kasiinoboonused

Veebipõhises mängukeskkonnas algab konto kasutamine tavaliselt registreerimisest. Kasutaja loob parooli, kinnitab e-posti aadressi ning tutvub vajaduse korral täiendavate turvaseadetega. Hiljem võib teenus pakkuda ka kaheastmelist autentimist.

Sarnaseid toiminguid kohtab veebikasiinode juures, kus registreerimise ja konto kasutamise tingimused sõltuvad konkreetsest platvormist. Näiteks Casino-latvia.com lehel saab tutvuda kasiinoboonuste liikide ja nendega seotud tingimustega. Konto turvaseadete kohta tuleb täpsemat teavet otsida valitud teenuse ametlikest juhenditest.

Mängukontoga võib olla seotud makseviis, mänguajalugu ja isiklikke andmeid sisaldav profiil. Seetõttu tasub juba registreerimise ajal vaadata, kas sisse saab logida täiendava kinnitusega.

Eriti mugav on see inimesele, kes kasutab sama kontot nii sülearvutis kui ka telefonis. Turvaseadete muutmisel võib teenus küsida uut kinnitust isegi siis, kui kasutaja on juba sisse loginud.

Mis muutus Smart-ID kasutamisel?

RIA uuendas 2026. aasta veebruaris riigi autentimisteenust, mille kaudu pääseb näiteks eesti.ee portaali ja Maksu- ja Tolliameti e-teenustesse. Uus Smart-ID+ lahendus seob sisselogimistoimingu kasutaja telefoniga.

Arvutis ilmub nüüd muutuv QR-kood. Selle lugemiseks tuleb avada telefonis Smart-ID rakendus ning valida QR-koodi skannimise võimalus. Pärast toimingu kinnitamist sisestatakse PIN1.

Telefonis toimub sama asi teisiti. Kui inimene avab e-teenuse mobiilibrauseris, saab ta valida Smart-ID rakenduse avamise. Rakendus käivitub otse ning sisselogimise saab lõpetada PIN1 sisestamisega.

RIA ametlik selgitus Smart-ID+ kasutuselevõtu kohta kirjeldab mõlemat võimalust. Uue lahenduse jaoks peavad telefoni operatsioonisüsteem ja Smart-ID rakendus olema ajakohased. Oluline on tähele panna, et muudatus puudutab riigi autentimisteenuses Smart-ID kasutamist. Muude veebikeskkondade sisselogimisvõimalused sõltuvad nende enda lahendustest.

PIN1 ja PIN2 täidavad eri ülesandeid

Smart-ID kasutamisel on kaks PIN-koodi, millel on erinev otstarve. PIN1 kinnitab inimese isikut sisselogimisel. PIN2 kasutatakse digiallkirjastamisel ja tehingute kinnitamisel.

Kui inimene avab hommikul Maksu- ja Tolliameti iseteeninduse, kasutab ta sisenemiseks PIN1. Dokumendi digiallkirjastamisel tuleb tavaliselt sisestada PIN2.

Telefoniekraanil tasub enne kinnitamist lugeda, millist toimingut parajasti tehakse. Ootamatult saabunud kinnitustaotlust ei ole põhjust heaks kiita.

Smart-ID+ QR-koodi skannimine on tasuta. RIA juhib tähelepanu ka sellele, et riigi e-teenustesse sisenemisel kasutatakse muutuvat QR-koodi, mis seob kinnituse konkreetse sisselogimisega.

Miks ühest paroolist alati ei piisa?

E-posti konto võib olla seotud kümnete teiste teenustega. Kui kasutaja unustab mõne mänguportaali parooli, jõuab lähtestamise link sageli just tema postkasti. Seetõttu väärib e-posti konto vähemalt sama hoolikat kaitset.

ITvaatlik soovitab kasutada igas keskkonnas eraldi tugevat parooli ning võimaluse korral kaheastmelist autentimist. Nende paroolide ja autentimise juhendis käsitletakse ka paroolihaldurite kasutamist.

Enne järgmise veebikonto loomist tasub mõned asjad läbi vaadata. Eriti puudutab see teenuseid, mida kasutatakse eri seadmetes. Kasulik kontrollnimekiri näeb välja selline:

- Erinev parool. Iga veebikonto saab oma salasõna, mida teistes teenustes ei kasutata.
- Teine kinnitusetapp. Võimaluse korral lülitatakse sisse autentimisrakendus või muu täiendav kontroll.
- Taasteandmed. E-posti aadress ja telefoninumber peavad olema ajakohased.
- Sisselogitud seadmed. Konto seadetes saab kontrollida aktiivseid seansse ja eemaldada vanu seadmeid.

Paroolihalduriga saab luua ka pikki juhuslikke paroole. Neid pole vaja eraldi meelde jätta, sest rakendus aitab salvestatud andmeid kasutada. Enamik paroolihaldureid võimaldab sisselogimisvälju automaatselt täita, mis teeb mitme veebikonto kasutamise mugavamaks. Peaparool peab aga olema tugev ja ainult selleks kasutatav.

Kaheastmelise autentimise korral küsib teenus lisakinnitust vastavalt oma turvareeglitele. See võib olla vajalik näiteks uues seadmes esmakordsel sisselogimisel.

Mida teha, kui uus sisselogimine ei tööta?

Smart-ID+ kasutamisel tasub alustada telefoni ja rakenduse uuendamisest. RIA juhiste järgi peavad need olema ajakohased ning mobiilibrauser peab uut lahendust toetama.

Kui arvutiekraanil olevat QR-koodi ei õnnestu lugeda, tuleb kasutada Smart-ID rakenduse enda skannimisfunktsiooni. Tavalise kaamerarakendusega tehtud toiming ei pruugi anda sama tulemust.

Telefonis aitab mõnikord brauseri seadete kontrollimine. RIA juhendab vältima Smart-ID+ kasutamisel privaatset sirvimisrežiimi ning määrama sobiva vaikebrauseri.

Mängu- ja meelelahutuskontodel võivad kehtida teistsugused juhised. Kui kinnituskood ei saabu või autentimisrakendus on vahetunud, tuleb kasutada

vastava teenuse ametlikku taastamisvõimalust.

Enne vana telefoni lähtestamist on mõistlik üle vaadata kõik olulised kontod. Nii saab kontrollida, kas vajalikud autentimisrakendused ja taastamisvõimalused töötavad ka uues seadmes.

- Uudised
- Sisuturundus

Pilt

