Mobiili ID võrdlus muude autentimismeetoditega

20. november 2023 - 1:04 Autor: AM

(Sisuturundus)

Digitaalajastul, kus enamik tehingud ja suhtlus toimuvad veebis, on mobiilne isikutuvastus ja digitaalne allkirjastamine muutunud igapäevaelu lahutamatuks osaks. Erinevad autentimismeetodid on selle protsessi keskmes, tagades, et elektroonilised toimingud oleksid turvalised ja usaldusväärsed. Traditsioonilised autentimismeetodid, nagu paroolid, PIN-koodid ja füüsilised ID-kaardid, on aastakümneid olnud standardiks, kuid nendega kaasnevad teatud riskid ja ebamugavused. Mobiil-ID on see-eest uuenduslik digitaalne autentimismeetod, mis on kujunemas tugevaks alternatiiviks, pakkudes kasutajatele uut turvalisuse ja mugavuse taset.

Mis on mobiili ID?

Mobiili ID on kaasaegne digitaalne isikut tõendav vahend, mis võimaldab isikul tõestada oma identiteeti elektroonilises keskkonnas ning allkirjastada dokumente ja tehinguid mobiilseadme kaudu. See on võrreldav digitaalse isikutunnistusega, mis on integreeritud kasutaja mobiiltelefoni ja on seotud konkreetse SIM-kaardiga. Mobiili ID allkirjastamine on võimalik mobiilioperaatori väljastatud spetsiaalse SIM-kaardi ja teenuse aktiveerimise tulemusena.

Mobiil-ID süsteem kasutab keerukaid krüptimise protsesse, et tagada edastatavate andmete turvalisus. See tähendab, et allkirjastatud dokumenti ei saa hiljem muuta ilma, et see muudaks allkirja kehtetuks, tagades nii dokumendi autentsuse ja terviklikkuse.

Meil Eestis, kus mobiil-ID on laialdaselt kasutusel, on see saanud oluliseks osaks digitaalsest infrastruktuurist, võimaldades kodanikel vaevata ligi pääseda e-teenustele. Mobiili ID abil saavad kasutajad hääletada e-valimistel, esitada maksudeklaratsioone, sõlmida lepinguid ja teha palju muid toiminguid, mis nõuavad õiguslikult sidumiseks identiteedi tõestamist ja allkirjastamist.

Mobiili ID on loodud olema platvormi- ja seadmeülene, mis tähendab, et seda saab kasutada erinevates seadmetes ja operatsioonisüsteemides.

Muud autentimismeetodid

Traditsioonilised autentimismeetodid on aja jooksul arenenud lihtsatest füüsilistest viisidest keerukate elektrooniliste süsteemideni, kuid enamik neist põhineb endiselt kolmel põhilisel autentimisfaktoril: midagi, mida kasutaja teab (näiteks parool või PIN-kood), midagi, mida kasutaja omab (näiteks ID-kaart), või midagi, mis on kasutaja füüsiline omadus (näiteks sõrmejäljetuvastuse või näotuvastuse puhul).

Paroolid ja PIN-koodid

Kõige levinumad ja traditsioonilisemad autentimismeetodid on paroolid ja PIN-koodid. Need on lihtsasti kasutatavad ja ei nõua täiendavaid seadmeid, kuid nende turvalisus sõltub suuresti kasutaja loodud parooli keerukusest ja konfidentsiaalsusest. Paroolide ja PIN-koodide probleem on see, et neid on suhteliselt lihtne ära arvata, eriti kui kasutatakse lihtsaid või korduvaid kombinatsioone.

Füüsilised autentimisvahendid

Füüsilised autentimisvahendid, nagu võtmekaardid, pangakaardid või ID-kaardid, on samuti laialt levinud. Need on tavaliselt seotud konkreetse kasutajaga ja nende kasutamiseks on tarvis füüsilist eset, mida peab autentimise ajal kaasas kandma. Kuigi see lisab turvalisusele kihi, on nende probleemiks see, et neid on lihtne kaotada või need võidakse varguse tulemusena kaotada.

Biomeetrilised meetodid

Biomeetrilised autentimismeetodid, nagu sõrmejälje- või näotuvastus, on muutunud üha populaarsemaks tänu nende võimele pakkuda unikaalset ja raskesti võltsitavat autentimist. Biomeetria kasutab inimese füüsilisi või käitumuslikke tunnuseid, et tuvastada isikusamasust. Need meetodid on üldiselt turvalisemad kui paroolid või PIN-koodid, kuid nende puhul võib olla probleemiks privaatsus või seadmete ühilduvus.

Turvalisus

Turvalisus on autentimismeetodite puhul üks olulisemaid tegureid. Mobiili ID pakub siin mitmeid eeliseid, kuna see tugineb kaheastmelisele autentimisele. See tähendab, et isegi kui üks turvaelement on võõrale isikule kättesaadav, ei ole süsteemi sisenemine võimalik ilma teise elemendita, mis lisab turvalisusele olulise kihi.

Lisaks sellele on mobiil-ID turvalisus tagatud ka täiustatud krüptimistehnoloogia abil, mis kaitseb kasutaja andmeid ja tehinguid.

Traditsiooniliste autentimismeetodite puhul, nagu paroolid ja PIN-koodid, on peamine turvarisk seotud nende ära arvamisega. Paroolide puhul on lisaks probleemiks ka see, et inimesed kipuvad kasutama lihtsaid ja kergesti meeldejäävaid kombinatsioone, mis muudab need kergesti haavatavaks. Füüsiliste autentimisvahendite ja biomeetriliste meetodite puhul on turvariskid seotud pigem seadmete kaotamise või varguse ning võltsimisega.

Kasutusmugavus

Kasutusmugavus on teine oluline aspekt, mida autentimismeetodite puhul arvesse tuleks võtta. Mobiil-ID puhul on kasutusmugavus tagatud sellega, et kasutajad saavad oma identiteeti tõendada ja tehinguid allkirjastada igal ajal ja igas kohas, kasutades selleks vaid oma mobiiltelefoni. See tähendab, et pole vaja meeles pidada keerulisi paroole või kanda kaasas lisaseadmeid. Mobiili ID abil autentimine on kiire ja lihtne.

Traditsiooniliste meetodite puhul võib kasutusmugavus olla piiratud. Näiteks paroolide ja PIN-koodide puhul võib tekkida vajadus neid tihti vahetada või meeles pidada mitmeid erinevaid kombinatsioone eri kontode jaoks. Füüsiliste autentimisvahendite puhul võib ebamugavus tekkida vajadusest neid pidevalt kaasas kanda ja riskist neid kaotada. Biomeetriliste meetodite puhul võivad kasutajad kogeda ebamugavust seoses oma privaatsusega või vajadusega kasutada spetsiifilist riistvara.

Ühilduvus ja integreeritavus

Mobiil-ID on loodud paindlikkust ja ühilduvust silmas pidades, et see sobiks sujuvalt erinevate platvormide ja süsteemidega. Tänu standardiseeritud protokollidele ja API-le (Application Programming Interfaces) saavad arendajad mobiili ID-d hõlpsasti integreerida erinevatesse veebi- ja mobiilirakendustesse, tagades, et kasutajad saavad oma identiteeti tõendada ja tehinguid allkirjastada ühtse ja turvalise protsessi kaudu.

Traditsiooniliste autentimismeetodite puhul võib ühilduvus ja integreeritavus olla keerukam. Näiteks füüsilised autentimisvahendid nagu ID-kaardid või pangakaardid nõuavad spetsiifilisi lugemisseadmeid ja ei pruugi olla ühilduvad kõigi süsteemidega. Samuti võivad paroolipõhised süsteemid nõuda erinevate turvanõuete ja protokollide järgimist, mis võib piirata nende integreerimist teiste süsteemidega.

Õiguslikud aspektid

Õiguslikud aspektid on autentimismeetodite juures kriitilise tähtsusega, kuna need määravad kindlaks meetodi kehtivuse ja usaldusväärsuse ametlikes toimingutes. Mobiili ID puhul on oluline märkida, et see on tunnustatud kui ametlik isikut tõendav dokument ja digitaalne allkirjastamise vahend. See tähendab, et mobiil-ID-ga allkirjastatud dokumendid on õiguslikult siduvad ja neil on sama juriidiline jõud kui traditsioonilisel paberil allkirjastatud dokumentidel.

Mobiili ID õiguslik tunnustamine on saavutatud tänu rangetele turvanõuetele ja standarditele, mis tagavad isikutuvastuse ja allkirjastamise protsesside usaldusväärsuse.

Traditsiooniliste autentimismeetodite puhul võivad õiguslikud aspektid olla keerulisemad. Kuigi füüsilised dokumendid ja allkirjad on üldiselt laialdaselt tunnustatud, võivad paroolide ja biomeetriliste andmete kasutamine tekitada õiguslikke küsimusi, eriti seoses andmekaitse ja privaatsusega.

- Uudised

- Sisuturundus