2FA beállítása a TTK levelezőrendszerben

A kétfaktoros hitelesítés beállításához szükség van tokenek (titkos kulcsból származtatott egyszeri kódok) generálásának a képességére. Bár ezt általában valamilyen hitelesítő szoftverrel szokták a felhasználók megoldani, legtöbbször app formájában az okostelefonon, számtalan cég gyárt célhardvert is erre a célra, amik pendrive vagy épp bankkártya méretűek is lehetnek.

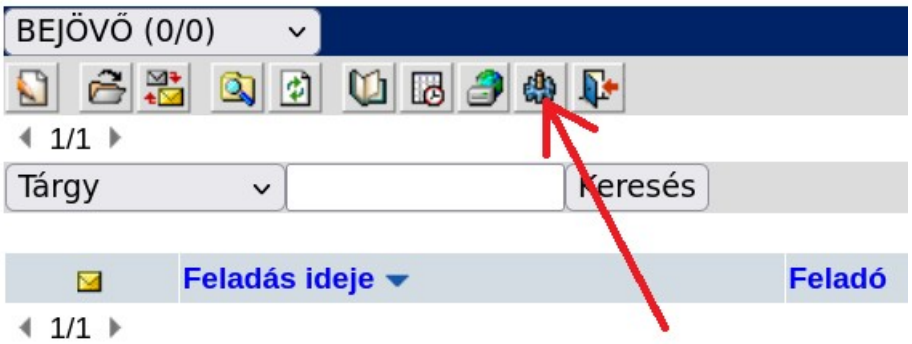
A hardveres token generálás előnye a szoftveres megoldással szemben, hogy a felhasználók által használt hitelesítő szoftverek sokszor ugyanazokon az eszközökön futnak, mint amikről a felhasználók bejelentkeznek a levelezésükbe, ezáltal pedig nem jön létre a kétfaktoros azonosítás legfontosabb célja, a faktorok fizikai szétválasztása. E nélkül pedig a 2FA korlátozottan tud csak további védelmet biztosítani a felhasználók levelezéséhez.

Szoftveres token generáláshoz például használható macOS és iOS alá az **Authy**, Windows alá a **FortiToken**, Linux alá az **OTPClient**, Android eszközökhöz pedig a **Google Authenticator**.

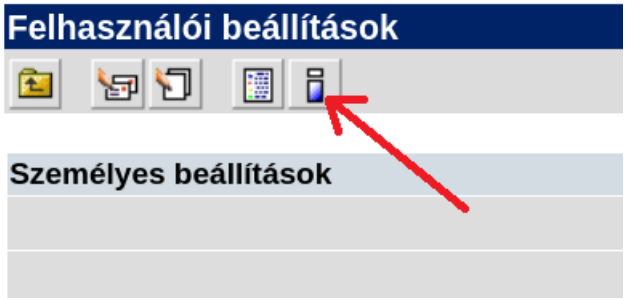
Amennyiben a felhasználó bármilyen szoftveres hitelesítő programot jelenleg is használ, a TTK levelezőrendszer kétfaktoros hitelesítésének a beállításához nem kell külön egy új szoftvert feltelepíteni. A meglévő is szinte biztosan használható.

1. A 2FA beállítása a klasszikus felületen:

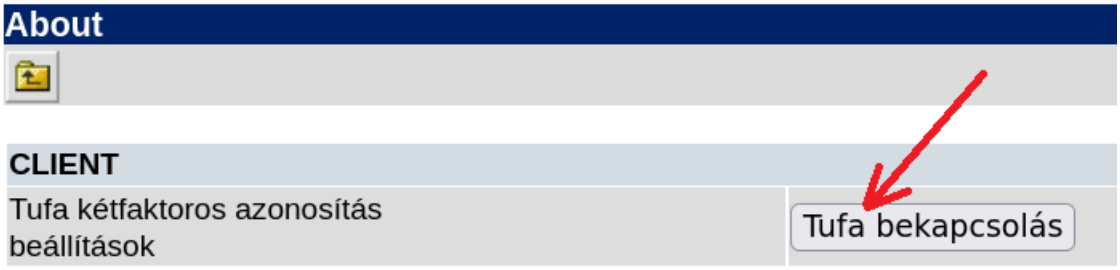
Belépés után a bal felső menüsorban a fogaskerék ikonra kell kattintani a beállításokba való belépéshez.



A beállításokon belül az **i** ikonra kell kattintani.



Itt található a kétfaktoros hitelesítés bekapcsolása a „Tufa kétfaktoros azonosítás beállítások” menüpontban.



A „Tufa bekapcsolás” gombra kattintva a felhasználó számára legenerálódik a kétfaktoros hitelesítés kulcsa, a QR-kód, és a csak egyszer felhasználható belépési kulcsok. Egy példa erre:

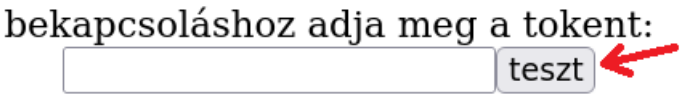
A felhasználó által választott hitelesítő alkalmazásban, például a Google Authenticator-ban, a kétfaktoros hitelesítés beállítható mind a beállító kulcs (a például szolgáló képen a „UMRQRVRHCMSE2RR5”) beírásával, mind a QR-kód beolvasásával.

Fontos, hogy amennyiben nem a QR-kódot használja a felhasználó, a beállító kulcs megadásánál ellenőrizni kell, hogy a kulcs típusa a hitelesítő (authenticator) szoftverben időalapúra (TOTP) legyen beállítva.

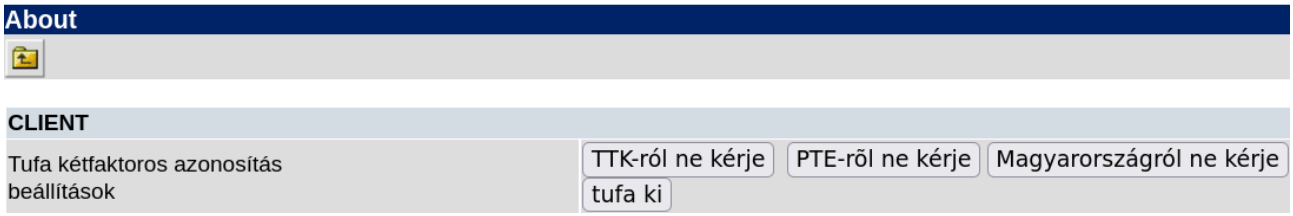
Pont amiatt, hogy a tokenek generálása a pontos idő aktuális értékét is igényli, miközben például az általános célú asztali számtógépek rendkívül megbízhatatlanok ezen a téren, ezért Windows és Linux operációs rendszerek alatt is érdemes egy időszerverrel a rendszeres időszinkronizációt bekapcsolni. Windows operációs rendszerek esetében a „Gépház” beállításain belül az „Idő és nyelv / Dátum és idő” alatt lehet az időszinkronizációt elvégezni, míg Linux alatt pedig ez parancssorból is megvalósítható.

A például szolgáló képen látható „Recovery kulcsok” kizárólag csak egyszer használhatók, kifejezetten arra szolgálva, hogy akkor is be tudjon lépni a felhasználó, ha a hitelesítő szoftver és az általa generálható tokenek például egy újratelepítést követően nem elérhetőek. Épp ezért nagyon fontos, hogy a felhasználó ezeket az egyszer használható kulcsokat lemásolja magának.

Miután a felhasználó sikeresen beállította a hitelesítő alkalmazásában a kétfaktoros azonosítást, legalulra a „bekapcsoláshoz adja meg a tokent:” mezőbe kell a legfrissebben generált tokent megadni, majd a teszt gombra rányomni.



Ennek sikeressége esetén a levelezőrendszerben a kétfaktoros azonosítás bekapcsolódik, hozzáférhetővé téve további beállítási lehetőségeket a „Tufa kétfaktoros azonosítás beállítások” menüpontban.



A „tufa ki” gomb kikapcsolja a kétfaktoros azonosítást, a felette lévő három gomb pedig arra szolgál, hogy a felhasználó beállíthassa azt az tartományt, amin belül egyáltalán nem szeretne a belépéskor kétfaktoros azonosításra szolgáló tokent is megadni. Mindhárom funkció bármikor tetszés szerint ki- vagy visszakapcsolható.

A „TTK-ról ne kérje” funkció a Természettudományi Kar vezetékes hálózatára és a PTE TTK Wi-Fi csatornára vonatkozik.

A „PTE-ről ne kérje” funkció a teljes egyetemi vezetékes hálózatra és a PTE területéről az Eduroam Wi-Fi csatornára vonatkozik.

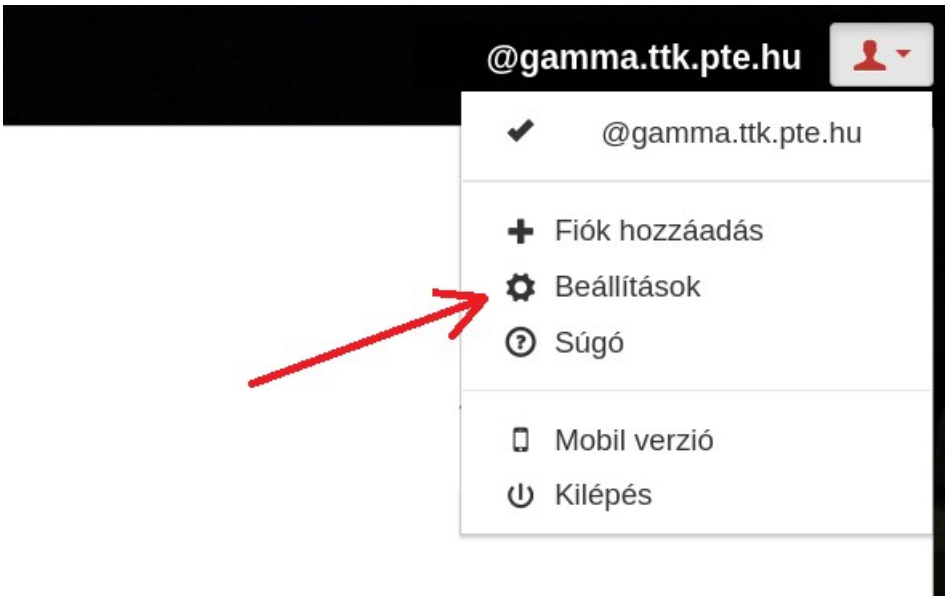
A „Magyarországról ne kérje” pedig bármilyen hazai helyszínről való bejelentkezésre vonatkozó funkció.

Ezekkel a funkciókkal sokkal könnyebbé válhat a kétfaktoros azonosítás használata a TTK levelezőrendszerben, mert például a „TTK-ról ne kérje” bekapcsolásával a Természettudományi Karon nem kell a tokenek állandó beírogatásával vesződni, miközben a kétfaktoros azonosítás továbbra is védi a felhasználó levelezését a külső támadókkal szemben.

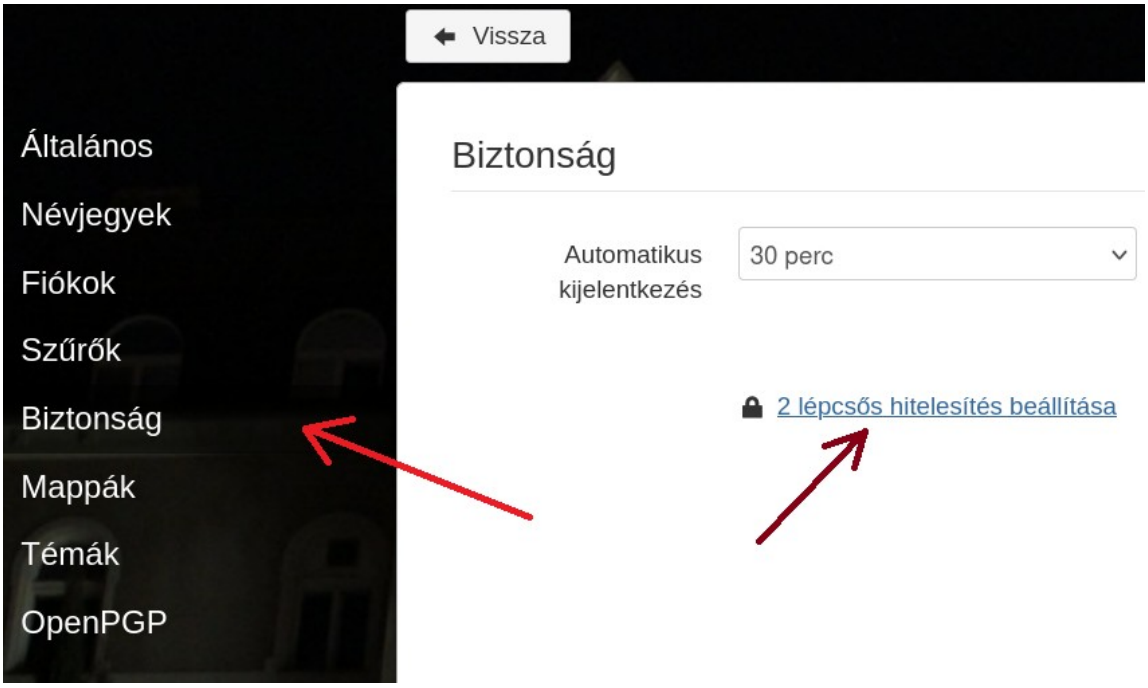
Ezen felül a klasszikus felület sikeres autentikáció esetén kilenc órán keresztül eleve nem kér újra tokent a felhasználótól belépéskor, ami így kényelmesen lefedhet egy átlagos munkanapot.

2. A 2FA beállítása a modern felületen:

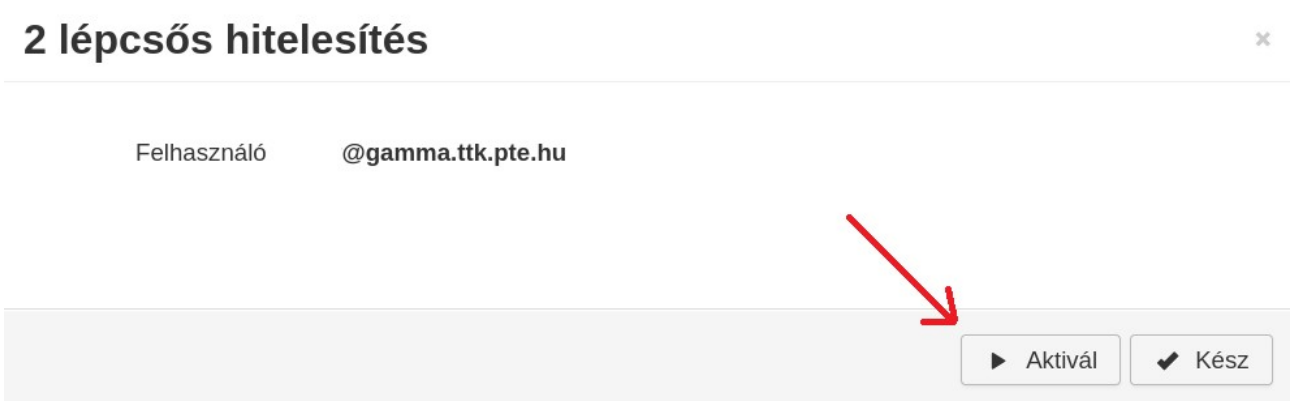
Belépés után a jobb felső profilképre kattintva a legördülő menüben a „Beállítások” lehetőséget kell kiválasztani.



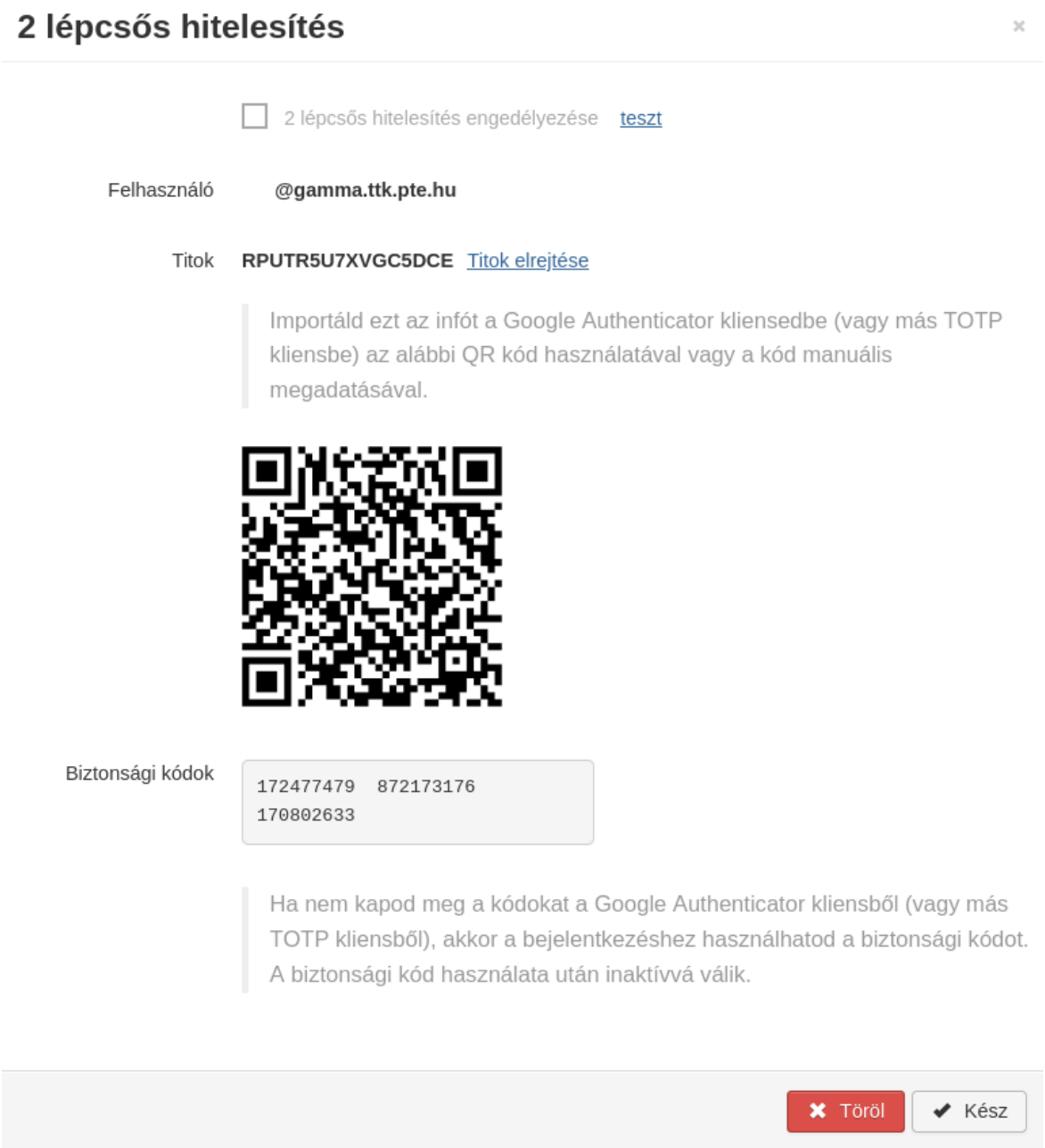
A beállításokon belül bal oldalon először a „Biztonság” menüpontra kell kattintani, majd jobb oldalon az ezáltal megjelenő „2 lépcsős hitelesítés beállítása” linkre kell kattintani.



A következő lépés az „Aktivál” gomb használata.



Az „Aktivál” gombra kattintva a felhasználó számára legenerálódik a kétfaktoros hitelesítés kulcsa, a QR-kód, és a csak egyszer felhasználható belépési kulcsok. Egy példa erre:



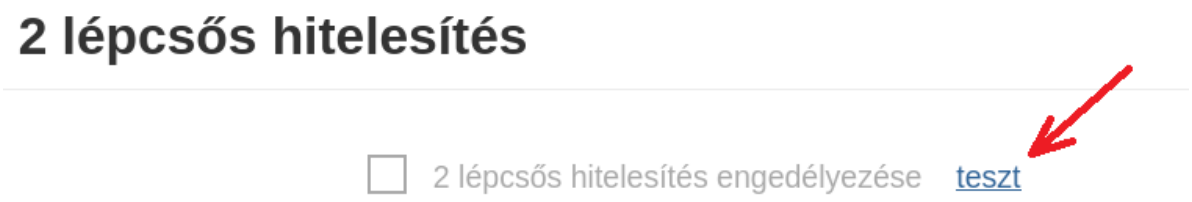
A felhasználó által választott hitelesítő alkalmazásban, például a Google Authenticator-ban, a kétfaktoros hitelesítés beállítható mind a beállító kulcs (a például szolgáló képen a „RPUTR5U7XVGC5DCE”) beírásával, mind a QR-kód beolvasásával.

Fontos, hogy amennyiben nem a QR-kódot használja a felhasználó, a beállító kulcs megadásánál ellenőrizni kell, hogy a kulcs típusa a hitelesítő (authenticator) szoftverben az időalapúra (TOTP) legyen beállítva.

Pont amiatt, hogy a tokenek generálása a pontos idő aktuális értékét is igényli, miközben például az általános célú asztali számtógépek rendkívül megbízhatatlanok ezen a téren, ezért Windows és Linux operációs rendszerek alatt is érdemes egy időszerverrel a rendszeres időszinkronizációt bekapcsolni. Windows operációs rendszerek esetében a „Gépház” beállításain belül az „Idő és nyelv / Dátum és idő” alatt lehet az időszinkronizációt elvégezni, míg Linux alatt pedig ez parancssorból is megvalósítható.

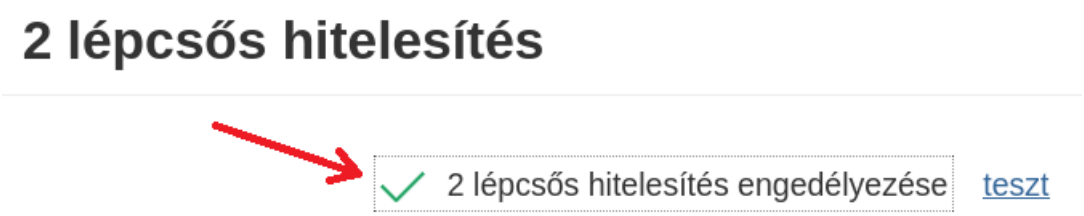
A például szolgáló képen látható „Recovery kulcsok” kizárólag csak egyszer használhatók, kifejezetten arra szolgálva, hogy akkor is be tudjon lépni a felhasználó, ha a hitelesítő szoftver és az általa generálható tokenek például egy újratelepítést követően nem elérhetőek. Épp ezért nagyon fontos, hogy a felhasználó ezeket az egyszer használható kulcsokat lemásolja magának.

Miután a felhasználó sikeresen beállította a hitelesítő alkalmazásában a kétfaktoros azonosítást, annak a levelezőrendszerben való élesítése előtt még tesztelnie kell azt, legfelül a „teszt” linkre kattintva.

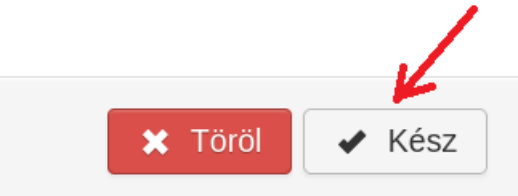


Amennyiben a felhasználó érvényes tokent írt be, a „Tesztelés” gombra kattintva az ki fog zöldülni.

Ezután egy nagyon fontos lépés következik. Innen egyet visszalépve be kell pipálni a „2 lépcsős hitelesítés engedélyezése” négyzetet.



Végül a lap alján a „Kész” gombbal aktiválható a hitelesítés.



Miután a felhasználó sikeresen bekapcsolta a kétfaktoros azonosítást TTK levelezőrendszer modern felületén, a következő bejelentkezéskor van lehetőség a „Két hétig ne kérje a kódot” mező bepipálására. Ez a funkció azonban kizárólag csak arra az eszközre vonatkozik, amin épp bejelentkezik a felhasználó.