



Erős, kétfaktoros felhasználó-azonosítási rendszer

Szeretné, ha az Ön jelszavait senki sem tudhatná meg?

Ha az Ön jelszava ellophatatlan, másokkal megoszthatatlan lenne?

Ha informatikai rendszerének jelszóvédelme egyes bankokénál is jobb lenne?

Szeretné mindezt a lehető legolcsóbban megkapni?

Ki tudhatja (meg) az Ön jelszavát?

Manapság nyilvánvaló, hogy a hétköznapi tevékenységünk során számos informatikai rendszert használunk jelszóval történő belépés után. Gondoljon csak bele,

- belépéskor a Windows indításakor a számítógépbe
- levelezőrendszer távoli elérésekor (webes levelező rendszerek használata)
- saját céges hálózat távoli elérésekor (VPN kapcsolat a cég irodai hálózatával)
- online megrendelések feladásakor (pl. vevői/partneri portálok, stb.)
- stb.

rende be kell jelentkeznünk egy-egy jelszóval (még akkor is, ha egyes esetekben a jelszót saját rendszergazdánk előre be is állította nekünk az adott rendszerhez, hogy ne kelljen kézzel beírni).

Sajnos a legtöbb esetben szokás szerint **állandó (ún. statikus) jelszavakat** használunk!

A statikus jelszavakat általában a rendszergazda állítja be, így akár meg is jegyezheti magának, és akárki nevében be is tud lépni az adott rendszerekbe – hogy csak egy hátrányát említsük.

Ha az Ön statikus jelszavát önmaga hozta is létre, és nem a rendszergazdája, a mai, nyilvánosan is elérhető kémprogramokkal és egyéb eszközökkel történő jelszólopás napjaink legnagyobb veszélyei – ráadásul jelszólopásra készült programokat korlátlanul az internetről is le lehet tölteni. Éppen ez indokolja erősen például a bankok vagy biztosítók esetében már jól ismert SMS jelszavak használatát.

Ha a jelszó nem biztonságos,...

...**bármilyen megtörténhet** – mint ahogyan sokakkal már meg is történt! Attól függően, hol használnak Önök még most is állandó jelszavakat, az érintett rendszerekben tárolt adatok, avagy azon rendszerek által biztosított szolgáltatások nincsenek teljes biztonságban!

Közismert egyszeri jelszavas megoldások

Statikus jelszavak helyett tehát olyan jelszavakat kell használnunk, melyek minden bejelentkezésnél megváltoznak: erre pedig az online banki rendszerekből már jól ismert, ún. **egyszeri jelszavak (One-Time-Password; OTP)** a legalkalmasabbak.

Ezeket a jelszavakat egy speciális háttérrendszer, az ún. **egyszeri jelszavas felhasználó-azonosító rendszer** érvényesíti a felhasználó bejelentkezésekor.

A jelszavakat a felhasználó több úton-módon kaphatja meg bejelentkezéskor:

- **SMS-ben** (lásd a legtöbb banki rendszer esetét) – ez azonban költséges, ráadásul a pontos költségek előre kiszámíthatatlanok, és az SMS-jelszót a telefonra küldés közben le is lehet hallgatni! (Minden bizonnyal ez az oka annak, hogy a bankok az SMS-jelszó költségeit rendszerint az ügyfélre hárítják át.)
- **Hardver eszközzel** a felhasználó saját maga állítja elő az egyszeri jelszót – a hardver eszközök (ún. **tokenek**) beszerzése rendkívül költséges, logisztikai szempontból rengeteg feladattal jár a kiosztásuk, cseréjük, „javításuk”, ugyanakkor könnyen otthon felejthetők, elhagyhatók, mely esetekben újakat kell vásárolni!

Egyedülálló mobil token technológia – az igazi megoldás!

A CIDWAY EGYEDÜLÁLLÓ MOBIL SZOFTVER TOKEN TECHNOLÓGIÁJA NAPJAINK LEGFEJLETTEBB ONE-TIME-PASSWORD (OTP) MEGOLDÁSA, AMELY ÖNMAGÁBAN SOFT-TOKENKÉNT, AVAGY BÁRMELY MOBIL ALKALMAZÁSBA INTEGRÁLVA BIZTONSÁGOS ÉS KÉNYELMES FELHASZNÁLÓ-AZONOSÍTÁST TESZ LEHETŐVÉ

A CIDWAY mobil token (vagy más néven soft-token, szoftver token) technológia egyik kiemelkedő előnye, hogy **nem tárolja** az egyszeri jelszó előállításához használatos személyes PIN kódot a mobil eszközön, így **visszafejthetlenné és kiemelkedően biztonságossá** teszi az alkalmazást még a mobil eszköz illetéktelen kezekbe kerülése esetén is. Ennek köszönhető továbbá, hogy **rossz PIN kód megadása esetén rossz egyszeri jelszó generálódik**, ám ezt csak a jelszót ellenőrző háttérrendszer kezelői tudhatják, a rossz jelszót előállító személy nem! E tulajdonságot kihasználva rossz jelszó érkezésekor a felhasználási területnek megfelelő **riasztások léphetnek életbe**.



Nollex Nemzetközi Kft.

A CIDWAY mobil token megoldás másik nagy előnye, hogy **az összes JAVA-képes telefontípust támogatja** - illetve az SDK segítségével akár **saját mobil alkalmazás védelmét** is megoldhatja vele.

A szoftver alapú token technológiának köszönhetően a CIDWAY mobil tokenek bevezetése és használata **rendkívül gazdaságos, gyorsan megtérülő** beruházás.



JELLEMZŐK

- **Erős OTP¹ azonosítási rendszer** – digitális tranzakció aláírásal kiegészített egyszeri jelszavas rendszer
- Személyes PIN kóddal védett, amely **PIN kódot a felhasználó önmaga bármikor megváltoztathatja!**
- **Nem tárolódik semmilyen bizalmas adat a felhasználó mobilján!**
- **100%-osan védett** a mobileszköz ellopása vagy elvesztése esetén is!
- **Teljes védelem**
 - **phishing** támadás,
 - **brute force** támadás,
 - **man-in-the-middle** támadás,
 - **PIN-jóslás** támadás,
 - **kód visszafejtés** ellen.
- **Klónozás elleni védelem:** rendszerdifferenciálás ügyfelek szerint (a tokenek csakis egy adott rendszerhez regisztrálhatók és csak azzal használhatók).
- **Offline is hitelesíthető OTP¹-t generál!** az online bejelentkezések és tranzakciók védelme mellett használja **fax, email, postai levél alapú megbízások felhasználó-azonosítására!**
- **Testre szabható** a cég image-nek megfelelő grafikákkal, színvilággal, nyelvezettel.
- **Örök életre szóló licencek** = minimális logisztikai feladatok

¹ One-Time-Password = egyszeri jelszó

CIDWAY hardver tokenek

A CIDWAY felhasználó-azonosítási rendszer az egyedülálló CIDWAY mobil token mellett számos egyszeri jelszót generáló hardver tokenet is támogat. A hardver tokenek kezelése szintén egyszerű, kinézetre pedig akár a céges megjelenéshez is igazodhatnak.

BANKKÁRTYA TOKEN



A hardveres token egy közismert, általánosan használt megoldás kétfaktoros felhasználó-azonosításra.

A Cidway **NagraID bankkártya hardver tokenek** előnye, hogy miközben nagyon egyszerű kezelni, **PIN kóddal védett** jelszó-generálást tesz lehetővé.

Mindössze pár milliméter vastag, hosszú élettartamú,

USB TOKEN



A **Cidway USB token** a legegyszerűbb, telepítés nélkül használható token bármely Windows / Macintosh / Linux / Solaris számítógéppel együtt biztonságos egyszeri jelszavak (one-time-password) generálására.

Az USB kulcson található gomb megnyomásával a

SESAMI SLIM TOKEN



A **Cidway Sesami hardver token** egy számológépre hasonlító, nagyon könnyen kezelhető token eszköz.

Az egyszeri jelszó előállítását ez esetben is a felhasználó **saját PIN kódja védi**.

A token védett a fizikai támadások ellen, hosszú élettartamú, és igény szerint a cég arculatához igazodva

bankkártyával megegyező méretű eszköz.

A bankkártya token a hátoldalán elhelyezkedő mágneses csík segítségével meg is személyesíthető.

generált egyszeri jelszó automatikusan a vágólapra, a legtöbb esetben pedig egyből a kurzor alatti aktív mezőbe kerül be.

A Cidway USB tokenek mérete rendkívül kicsi, mindössze 18 x 45 x 3 mm és súlya csupán 2,5 gramm.

Mindezek mellett a Cidway USB token **védett a token fizikai támadása ellen, hermetikailag zárt, vízálló, elem-, LCD- és mozgó alkatrész-mentes.**

grafikázható.

A **2 soros LCD** kijelzős token mindössze 3,2 mm vastag és bankkártya méretű.

Hexadecimális vagy decimális jelszavakat képes generálni.

További információk

A CIDWAY egyszeri jelszavas felhasználó-azonosítási rendszerről a www.cidway.hu oldalon olvashat.

Kérdéseivel kapcsolatban szívesen állunk rendelkezésére elérhetőségeinken.

