CIDWAY ismertető

CIDWAY One-Time-Password (OTP) rendszer

Axico Kft. 1139 Budapest, Frangepán u. 11. Tel:+36-1-450-2970 Fax: +36-1-351-2576
www.axico.hu e-mail: uzletimegoldasok@axico.hu

A CIDWAY ONE-TIME-PASSWORD (OTP, EGYSZER HASZNÁLATOS JELSZÓ) RENDSZER

A CIDWAY SESAMI OTP RENDSZER FŐBB JELLEMZŐI

- **Erős OTP azonosítási rendszer.**
- Kényelmes, könnyű használat – a saját telefonja/PDA-ja mindenkinek mindig kéznél szokott lenni.
- **Időkorlát nélküli licencek –** alacsony fenntartási költség.
- „Token-pool" licencelés: rugalmas token licencgazdálkodás (a visszavont token licencek biztonságosan, szabadon újra kioszthatók).
- Vegyes autentikációs szerver működés támogatása (Mobil, SMS és hardveres tokenek egyszerre történő kezelése egyetlen autentikációs szerverrel).
- **A felhasználói OTP érvényessége offline, időben visszamenőleg is ellenőrizhető.** Így lehetséges például az OTP-vel „aláírt" faxok vagy csekkek hitelesítése is.
- **Rendszerdifferenciálás** CIDWAY-t használó cégek szerint (a tokenek csakis egy adott rendszerhez regisztrálhatók, és csakis az adott rendszer képes érvényesíteni az általuk generált OTP-ket).
- A szervezeti igények szerint **skálázható**.
- Bármely **LDAP v3 kompatibilis** címtárral azonnal integrálható (pl. Microsoft AD és LDS, vagy OpenLDAP 2.4). Egyéb integrációs igény esetén egyedi fejlesztés igényelhető.
- **Desktop Login** for Mac, Unix & Windows XP/Vista/7 támogatás.
- **RSA és egyéb autentikációs szerverrel párhuzamos működés** támogatása (ha létezik már kiépített azonosítási rendszer, amiről áttér vagy amely mellett a CIDWAY-t bevezeti).
- Webes felületű, többszintű jogosultság alapú adminisztráció (6 adminisztrációs jogosultsági szint).
- Egyszerű tömeges token menedzsment egyetlen konzolból.

A CIDWAY SESAMI OTP RENDSZER FŐBB ALKOTÓRÉSZEI

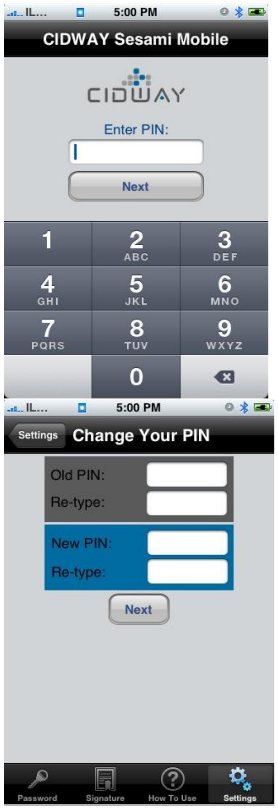
- **CIDWAY GAIA AUTHENTICATION SERVER**: a CIDWAY Sesami rendszer által támogatott hardver, SMS és Mobile token által generált OTP-ket képes párhuzamosan érvényesíteni **online vagy offline**. A szerver oldali komponens ezen felül számos backoffice/helpdesk funkciót is tartalmaz, például az offline OTP hitelesítést vagy a backup SMS OTP kiküldését bármely telefonszámra (arra az

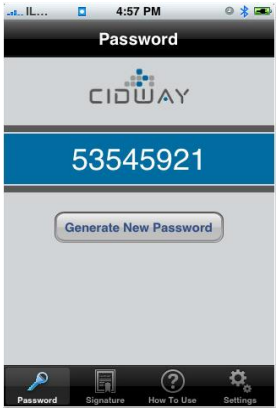
esetre, ha valaki mégis otthon hagyta volna mobileszközét), stb. Az azonosításhoz használatos OTP-k érvényességi ideje rendkívül rugalmasan paraméterezhető.

- **CIDWAY SESAMI SMS GENERATOR**: sikeres felhasználó-azonosítás után kiszámítja az idő alapú OTP-t, amely aztán SMS-ben kerül elküldésre a felhasználó mobiltelefonjára.

A CIDWAY SESAMI OTP RENDSZER ÁLTAL TÁMOGATOTT TOKENEK

- **CIDWAY SESAMI MOBILE TOKEN**: JAVA alapú OTP generátor szoftver, amelyet a felhasználó mobil eszközére kell telepíteni és első használat előtt a háttérrendszerrel regisztrálni. A kezdeti regisztráció után bármikor offline, külön költség nélkül, közvetlenül a mobil telefonjukon vagy PDA-jukon generált, másodperc alapú OTP segítségével korlátlan számú alkalommal azonosítsák magukat.





JELLEMZŐK

- **Erős OTP azonosítási rendszer – akár digitális tranzakció hitelesítéssel kiegészítve.**
- **Nem tárolódik semmilyen bizalmas adat a felhasználó mobilján!**
- **100%-osan védett a mobileszköz ellopása vagy elvesztése esetén is!**
- **Védelem**
  - phising
  - brute force
  - man-in-the-middle
  - PIN jóslás
  - kód visszafejtés

  támadások ellen.
- **Klónozás elleni védelem:** rendszerdifferenciálás ügyfelek szerint (a tokenek csakis egy adott rendszerhez regisztrálhatók és csak azzal használhatók).
- A felhasználó a saját mobiltelefonjára/PDA-jára telepített, JAVA alapú szoftver (soft token) segítségével **offline** (mindennemű kapcsolat vagy SMS nélkül) generálja az azonosításához szükséges OTP-t – **adathalászat (pl. phising, man-in-the-middle támadások) elleni védelem**.
- **Az iparágban egyedi „stressz-OTP”**-k előállítása: mivel a mobil eszközben nem tárolódik a felhasználó PIN kódja, csupán egy OTP-számolási algoritmus, így az algoritmussal (a szoftverrel) felhasználó **helytelen** PIN kóddal is tud OTP-t generálni. A helytelen PIN kóddal generált OTP-t, stressz-OTP-nek nevezzük, melyet a **CIDWAY GAIA AUTHENTICATION SERVER** érvénytelen azonosításnak értékel. Egyedi fejlesztéssel stressz-OTP-k észlelése estén egyéni műveletek hajthatók végre.
- A mobil token biztonságos, többlépcsős, de ugyanakkor rendkívül gyors és egyszerű, online vagy személyes regisztrálás után vehető csak használatba.
- **Többfajta online/offline OTP-továbbítási csatorna támogatása a hitelesítést kérő felé (web űrlap, FAX, SMS, WAP, MMS, GPRS, hang)**

- Mobil tranzakciós szoftverekbe integrálható (pl. mobil banki szolgáltatások, hűségprogram alkalmazások)
- A felhasználó bármikor használatba vehet egy új mobiltelefont, feltéve, hogy az arra újonnan telepített mobil tokent az első használat előtt a rendszerben regisztráltatja.
- Testre szabható mobil token szoftver képernyők (céges logo és színvilág használata lehetséges).
- A felhasználó a regisztráció során önmaga által választott PIN kódjával generálja az OTP-t.
- A felhasználó **bármikor** egyszerűen megváltoztathatja saját PIN kódját mindennemű kapcsolat nélkül a saját telefonján/PDA-ján.
- A generált OTP **másodperc alapú**.
- **A felhasználói PIN-t nem tárolja és nem továbbítja a mobil eszköz!**
- **Automatikus, transzparens időszinkronizálás** az autentikációs szerverrel.
- Kétirányú felhasználó-azonosítás weboldalakon.
- **A legszélesebb körű mobiltelefon/PDA operációs rendszer támogatása:** gyakorlatilag a ma használatos mobiltelefonok mindegyike, amin JAVA alkalmazás futtatható:

- **CIDWAY SESAMI SMS TOKEN**: minden egyes személynek, akinek SMS OTP hitelesítést szeretnénk nyújtani szükséges egy-egy SMS token, amelynek segítségével az SMS generátor legenerálja az OTP-t, majd az autentikációs szerver ez alapján ellenőrizni tudja a személy-token-OTP hozzárendelést. A felhasználók ez esetben közvetlenül a mobileszközükre SMS-ben kapott, előre meghatározott ideig érvényes OTP segítségével azonosítják magukat. A felhasználók mobileszköze így olyan virtuális tokenként működik, amelyre nem kell külön szoftveres tokent vagy egyéb modult telepíteni vagy regisztrálni. **A CIDWAY licencelési politikájának köszönhetően a Sesami SMS Token licencek díjmentesen járnak a Sesami Mobile Token licencek mellé.**

JELLEMZŐK

- A felhasználók a saját mobiltelefonjukra kapott, előre meghatározott ideig érvényes OTP segítségével azonosítják magukat.
- Bármilyen, SMS üzenetek fogadására alkalmas mobiltelefonnal, PDA-val vagy egyéb eszközzel használható.
- Az OTP-t a **SESAMI SMS GENERATOR SERVER** generálja és küldi ki a megadott SMS gatewayen keresztül (ha létezik, a már használatban lévő SMS gatewayhez integrálható).
- Nem tárolódik az OTP generálásához használatos bizalmas adat a felhasználó mobil eszközén, a kiküldött SMS-OTP csak egyszeri alkalommal használható azonosításra.
- A felhasználói oldalon nincs szükség szoftver telepítésére vagy regisztrálására a használatához.
- A felhasználó bármikor azonnali használatba vehet egy új mobiltelefont, feltéve, hogy nem változtatja meg a telefonszámát.
- A **SESAMI SMS GENERATOR SERVER**-hez küldött kérés váltja ki a az SMS-OTP generálását és kiküldését. A kérést a felhasználó több módon is kezdeményezheti, például:
    - A felhasználó beírja login nevét és statikus jelszavát egy pre-autentikációs weboldalon, amely kiváltja a kérés elküldését a

CIDWAY SMS-OTP Generator Serverhez.

- A felhasználó megadja login nevét és statikus jelszavát egy tűzfal által kezdeményezett kihívás-válasz (challange-response) alapú felhasználó-azonosítási folyamat során, ami továbbküldi a kérést a CIDWAY SMS-OTP Generator Serverhez.
- A felhasználó által beküldött SMS váltja ki az SMS-OTP generálását a CIDWAY SMS-OTP Generator Server részéről. Az SMS-OTP kérő üzenet protokoll többféle módon is létrehozható:
    - A felhasználó által küldött üzenetet lehet akár üres is. Egy üres SMS üzenet elküldésével a felhasználó automatikusan egy SMS-OTP-t kap.
    - A felhasználó üzenete tartalmazhat egy tetszőleges karaktersort, például a következőt: "OTP".
    - A felhasználó üzenete összetettebb is lehet, és tartalmazhatja a felhasználó PIN-jét, amely így erősebb autentikációt tesz lehetővé az OTP-Generator Serveren. Például a következő karaktersor: "OTP4586" tartalmazza a felhasználó PIN-jét. A szerver képes ellenőrzi a felhasználói PIN-t, mielőtt legenerálja az SMS-OTP-t és kiküldi azt. A biztonság növelése érdekében lehetőség van arra is, hogy a felhasználók SMS-ben tetszés szerint kezdeményezhessék a PIN-jük megváltoztatását.

Megjegyzés: *a mobilszolgáltatónál felmerülő SMS-küldési költségeket számításba kell venni az SMS-OTP rendszer tervezésekor. A CIDWAY rendszer mellé világszinten egyedülálló szolgáltatási minőséget nyújtó (nem hazai telekommunikációs cégen keresztül működő) SMS-szolgáltatást tudunk biztosítani, amely rendszerrel a CIDWAY külön üzembe állított SMS gateway hardver nélkül (HTTPS csatornán keresztül) képes együttműködni.*

SMS költségek felszámítása a felhasználóknak

A CIDWAY GAIA Server egy speciális kiegészítő modulja képes folyamatosan számolni a felhasználó részére kiküldött SMS--OTP-k számát. A kiküldött SMS–OTP-ket sávosan és kiküldés alapján is lehet figyelni. Ez lehetővé teszi, hogy az SMS-OTP-ket előre meghatározott feltételek teljesülésekor a kiküldött darabszám alapján, felhasználónként kiszámlázzák (pl. egy adott felhasználónak a havi x db feletti darabszámot).

Ez a modul jellemzően összekapcsolható back-office rendszerekkel (vagy bármilyen számlázó és jelentéskészítő eszközzel), lehetővé téve ezzel, hogy igény szerint elkönyveljék és kiszámlázzák az SMS-OTP-k költségeit. Az összekapcsolási interface általában olyan standard protokollokat használ, mint a SOAP, az XML stb. Mindezek mellett ad-hoc interface (pl. egyszerű fájl vagy adatbázis lekérdezés) kifejlesztésére is lehetőség van, amennyiben erre igény mutatkozik.

- **CIDWAY HARDVER TOKENEK**:
  - **CIDWAY Sesami SLIM**

- Hordozható és robusztus (**3,2 mm vastag – bankkártya méretű**)
- 2 soros LCD kijelző
- Cserélhető elem (a token adatai nem törlődnek elemcserekor)
- Idő alapú OTP – **másodpercenként** új OTP generálása
- **8 karakter hosszú OTP** generálása (hexadecimális vagy decimális)
- Az eszközt a felhasználó által választott PIN védi (beállítható 0-15 próbálkozási lehetőség)
- Védelem a token fizikai támadása ellen
- Védelem a felhasználó fizikai kényszerítése esetén is (stressz PIN kód)
- Nem kell hozzá kártyaleolvasó vagy más, hasonló eszköz
- Testre (cégre) szabható előlap grafika
- 1-3 év választható garanciaidő
- **Alacsony fenntartási költség**

  - **NagraID Display Card 306e**

- Métretek: 85.5mm x 54mm x 0.8mm
- NagraLam laminálási technológiával készül
- OTP OATH algoritmus használata
- **Dinamikus, 6 karakter hosszú OTP** generálása
- Számos standardnak megfelel (ISO/IEC, INCITS, ANSI, CQM és egyéb függőben lévő minősítések)
- Védelem a token fizikai támadása ellen
- Testre (cégre) szabható grafika

- Kártya megszemélyesítési lehetőség
- 1-3 év választható garanciaidő

- **YubiKey USB One-touch token**

- 18 x 45 x 3 mm USB kulcs kialakítás (2,5 gramm)
- OTP OATH algoritmus használata
- **Dinamikus OTP** 6-8 jegyű generálása gombnyomásra
- **Automatikus OTP beillesztés az aktív mezőbe**
- **AES-128 titkosítás**
- **Platform-független**, támogatott rendszerek:
  Windows 98SE és későbbi
  MacOS 9 és későbbi
  Linux és Solaris USB HID támogatással (standard USB driver)
  más rendszerek standard USB hosttal
- Számos standardnak megfelel (ISO/IEC, INCITS, ANSI, CQM és egyéb függőben lévő minősítések)
- Védelem a token fizikai támadása ellen
- Hermetikailag zárt, vízálló
- Elem-, LCD- és mozgó alkatrész-mentes
- Színválaszték
- Egyedileg logozható

KEDVEZŐ LICENCELÉS

A CIDWAY Sesami OTP rendszer árazásában kizárólag a megrendelt tokenek száma játszik szerepet, azaz a szerver komponensekért NEM kell külön licencdíjat fizetni.

„Token-pool" licencelés mobil/SMS tokenek esetén: rugalmas token licencgazdálkodás (a felhasználóktól visszavont token licencek biztonságosan, szabadon és azonnal újra kiosztathatók, nem kell a felhasználóktól „visszakérni") – ergo a megrendelt token pool által biztosított mennyiségi keretek között a token licencek bármikor szabadon – akár a felhasználóval történő egyeztetés nélkül – átruházhatók más felhasználókra.

A licenc díja a következőket tartalmazza:

- **CIDWAY GAIA AUTHENTICATION SERVER** licenc
  - A klaszterek és a backup szerverek számától függetlenül csak egyetlen licenc beszerzésére van szükség – a licenc maga korlátlan időre érvényes, nem lejáró időtartamú licenc.
  - A CIDWAY GAIA autentikációs szerverhez rendelhető olyan modult, amely segítségével SMS OTP-k kiküldésekor a felhasználó saját számlájára terhelhető a megadott számot meghaladó SMS-ek díja (amennyiben létezik a az adott cégnél számlája, pl. pénzintézetek, szolgáltató cégek esetében).
- **CIDWAY SESAMI SMS GENERATOR** licenc
  - Mobil és SMS tokenek mellé ingyenes, hardver tokenek mellé nem jár (mivel nem is szükséges).
- **CIDWAY Token licencek** a megrendelt darabszámban
  - **Mobil tokenek**
    CIDWAY SMS egyszeri jelszavak kiküldéséhez szükséges licencek.
    A CIDWAY Sesami Mobile Token licencelési szabályaiból következően ezen mobil token licencek mellé automatikusan díjmentesen jár a CIDWAY **SMS alapú OTP** generátor rendszerének licence is, amely adott esetben megfontolhatóvá teszi az esetlegesen már jelenleg használatban lévő SMS OTP kiküldő rendszer kiváltását és ezzel a jelenlegi éves licenc- és karbantartási díjak megtakarítását is.

    A speciális licencelésnek köszönhetően a megrendelt mobil token felhasználószámon belül a felhasználóknak szabadon választhatóan vagy a mobil vagy az SMS token használata állítható be és a két fajta token rendszer használata között bármikor egyszerűen és gyorsan lehetséges váltani.
  - **SMS tokenek**

CIDWAY SMS egyszeri jelszavak kiküldéséhez szükséges licencek.

- **Hardver tokenek**

  CIDWAY hardver token használatához szükséges eszközök és licencek.

- Alapszintű technikai támogatás

ÉVES KARBANTARTÁS

A CIDWAY Sesami OTP rendszer licencei mellé éves karbantartási szolgáltatási díj mellett a következő szolgáltatásokat nyújtjuk:

- szerver és token szoftverfrissítések, hibajavítások, új GUI fejlesztések elérhetősége
- új támogatott platformok használatának lehetősége (pl. újfajta mobil eszközök vagy szerver op. rendszerek)
- standard (vagy egyéb megrendelt) technikai támogatás

Az első beszerzés automatikusan tartalmazza az első évre szóló karbantartási szolgáltatási díjakat.

A karbantartási szolgáltatás lejártával a fenti szolgáltatások nem vehetők igénybe.

Átmenetileg felfüggesztett karbantartási szolgáltatási időszak a későbbiekben az elmaradt időszakra járó karbantartási szolgáltatási díjak megfizetése mellett folytatható.

TOVÁBBI INFORMÁCIÓK

Honlap és elérhetőségek: www.cidway.hu