Cardinal
Számítástechnikai Kft.
1025 Budapest, Pusztaszeri út 91. +36 1 345 7980 http://www.cardinal.hu

ViCA alkalmazás

Termékismertető

(ViCA 2.0)

Verzió: 1.0

2020. május

Tartalomjegyzék

1. Összefoglaló

A ViCA (Virtuális Chipkártya Alkalmazás) a Cardinal Kft. korszerű mobil hitelesítési eszköze, mely támogatja az Európai Unió PSD2 Irányelv szabályozás-technikai standardja (EBA-RTS) által megkövetelt **kétfaktoros**, **erős ügyfél-hitelesítési eljárás** (SCA) követelményeit. Az alkalmazás **Android**, **iOS** valamint **Windows** platformon érhető el.

A Pénzforgalmi szolgáltatás nyújtásáról szóló 2009. évi LXXXV. Törvény előírja, hogy a pénzforgalmi szolgáltatók 2019.09.14-től Magyarországon is erős ügyfél-hitelesítést (SCA) kötelesek alkalmazni, ha a fizető fél fizetési számlájához online módon fér hozzá, illetve a számlán elektronikus fizetési műveletet kezdeményez.

Mobiltelefon – a személyes hitelesítés eszköze

A Cardinal által kifejlesztett Virtuális Chipkártya Alkalmazással (ViCA) a mobiltelefonok **személyes hitelesítési eszközként** is használhatók. Az alkalmazás kétfaktoros (jelszóval védett, futtató mobil eszközre vagy Windows desktopra telepített) erős (**RSA, PKI technológiára épülő**) felhasználói azonosítást és hitelesítést tesz lehetővé. A ViCA segítségével a telepített Electra Ügyfélprogram, az Electra Internet Banking és Mobil Banking, valamint a MobilApp alkalmazások **aláíró kulcspárokat és tanúsítványokat tudnak generálni**, illetve regisztrálni az Electra rendszer használatához. A tanúsítvány használatával a felhasználók biztonságos módon tudnak az Electra alkalmazásokba bejelentkezni, és a kliens felületeken rögzített megbízásaikat elektronikusan aláírni, hitelesíteni.

A ViCA-t összehasonlítva az egyéb hitelesítési eljárásokkal a chipkártyától eltérően az akkor is használható, amikor a felhasználó a bank szolgáltatásait mobiltelefonról vagy táblagépről veszi igénybe. Míg az SMS-ben küldött jelszó egy egyszeri hitelesítési kódot tartalmaz, addig a ViCA a felhasználó privát kulcsával végzi el a megbízások aláírását. Az applikáció szabványos, könnyen auditálható eszközökkel és algoritmusokkal dolgozik (RSA, SSL, PBKDF2).

Dinamikus összekapcsolás

Az alkalmazás használata támogatja a **PSD2 Irányelvben** meghatározott „dinamikus összekapcsolás” feltétel teljesülését a bankba benyújtandó tranzakciók jóváhagyási, hitelesítési folyamatában.

Biometrikus azonosítás

Az Android és az iOS operációs rendszert futtató ViCA applikációkban lehetőség van biometrikus azonosításra is (ujjlenyomat). Az azonosításnak ezt a módját választva az alkalmazás indításakor nem szükséges a ViCA jelszó megadása, helyette az **adott eszköz és operációs rendszer által biztosított biztonságos biometrikus azonosítást** lehet igénybevenni.

ViCA Mikro Szerver

A PSD2 szabályozás szélesebb körű kielégítését biztosítja **az alkalmazás önálló szerveres változata**: a ViCA Mikro Szerver. Ez lehetővé teszi, hogy a bankok a PSD2 Irányelv szigorú hitelesítési eljárását támogató alkalmazást ne csak az Electra rendszerhez tudják felhasználni, hanem a szolgáltatás a **bank minden olyan feldolgozó rendszere számára is elérhető legyen**, ahol a hatályos törvények vagy a bank belső szabályozása erős ügyfél-hitelesítési eljárást követelnek meg.

A ViCA push üzenetküldő funkciójának működéséhez az önálló ViCA Mikro Szerver telepítésére van szükség.

Egy applikáció – több bank felé

Adott felhasználó által beregisztrált ViCA alkalmazás magához a felhasználóhoz kötődik és nem az adott bankhoz, így azt egyszerre több bank Electra rendszerébe is be lehet regisztrálni. Futása közben az applikáció a már regisztrált bankokkal párhuzamosan tudja tartani a kapcsolatot, így több banki kapcsolat egyszerre történő használata közben a felhasználónak nem kell az egyes bankok között folyamatosan váltogatni. A ViCA alkalmazásban az egyes bankokból érkező üzenetek az **adott bank egyedi arculatának megfelelően** jelennek meg az alkalmazást futtató eszköz képernyőjén.

Push érteítések és üzenetküldés

A ViCA üzenetek fogadására is alkalmas, melyek érkezhetnek a bank Electra rendszeréből vagy megfelelő **API-n keresztül egyéb banki rendszerekből** is. (pl. banki számlaegyenleg értesítések, marketing célú – célzott felhasználónak címzett üzenetek). A beérkezett üzeneteket a ViCA alkalmazás titkosítva tárolja. A szolgáltatás biztosításához ViCA Mikro Szerver előzetes telepítése szükséges.

Kétcsatornás autentikáció

A ViCA alkalmazás egyik legnagyobb erőssége, hogy az Internet- vagy Mobil Bankingtől független, **önálló kommunikációs csatornát nyit a bank felé**. Így egy Internet-, vagy Mobil Banking kapcsolatot célzó hacker támadás esetén a ViCA alkalmazás és a bank közötti kapcsolat továbbra is biztonságos marad.

A kétcsatornás autentikáció, a **nyilvános kulcsú infrastruktúra (PKI) használata** mellett tovább erősíti a felhasználók biztonságát. A ViCA használatával nincs szükség jelszavakra, token kódokra, melyeket adathalász támadással meg lehet szerezni.

Az alkalmazás lehetőséget ad arra is, hogy a közbeékelődéses (pharming) támadásokat detektálni lehessen.

Költséghatékonyság

A ViCA alkalmazást használva **megszűnik az SMS küldés költsége** mind a banki rendszerbe való bejelentkezési folyamat, mind egy adott megbízás aláírási folyamata során. Azzal, hogy a ViCA alkalmazás a felhasználó saját eszközén fut, a **banknak nem kell további kellékeket, infrastruktúrát** (tokeneket, chipkártyákat és kártyaolvasókat) **beszereznie és karbantartania.**

A ViCA push üzenetküldő funkciója lehetővé teszi, hogy a bank az egyéb, jelenleg jellemzően SMS-ben küldött **banki információkat** (pl. tranzakciós értesítések, napi egyenleg, kártyőr, számlaőr, banki terméktájékoztatók, promociós kampányok üzenetei, stb.) **biztonságos csatornán, egyéb költségek nélkül juttassa el a felhasználókhoz.** A bankok így jelentős költségmegtakarítást érhetnek el azáltal, hogy a különböző értesítéseket SMS helyett ViCA-n keresztül juttatják el.

Kinek érhető el a szolgáltatás?

Az alkalmazás önállóan nem használható internet bankoláshoz, meglévő Internet vagy Mobil Banking szolgáltatás szükséges hozzá. Annak használatát a bankkal kötött szerződés alapján a bank rögzíti a felhasználó által igénybe vett elektronikus csatorná/k/hoz.

Az alkalmazás Androidos operációs rendszerű mobil eszközökhöz a **Google Play** szolgáltatásból, Apple iOS operációs rendszerhez az **App Store-ból**, míg a Windowsos rendszerekhez a **Microsoft Store-ból** tölthető le.

2. A ViCA alkalmazás működése

A virtuális chipkártya alkalmazással (ViCA) a mobiltelefon, illetve Desktop ViCA alkalmazás esetén az adott asztali számítógép egy személyes hitelesítési eszközzé válik. Az alkalmazás segítségével az Electra Ügyfélprogram, az Electra Internet- és Mobil Banking, valamint az Electra MobilApp csatornák felhasználói aláíró kulcspárokat és tanúsítványokat tudnak generálni és beregisztrálni az Electra rendszer használatához, melyek használatával számlavezető bankjuk felé küldendő megbízásaikat biztonságos módon tudják hitelesíteni.

A **ViCA alkalmazás** egyszerre több bank Electra rendszerébe is regisztrálható. Az alkalmazás futása közben az minden beregisztrált bankkal párhuzamosan tartja fenn a kapcsolatot, így a felhasználók nem kényszerülnek arra, hogy használata közben az egyes bankok között autentikációs eszközöket kelljen váltogatni. Minden egyes bankból érkező üzenet az adott bank arculatának megfelelően kerül megjelenítésre.

Biztonsági szempontból a ViCA alkalmazás az SMS jelszavas és a chipkártyás hitelesítés között helyezkedik el. Az SMS jelszavas aláírásnál erősebb és költséghatékonyabb, míg a chipkártyás aláírásnál ugyan gyengébb, de sokkal szélesebb körben felhasználható.

A **chipkártyával** összehasonlítva a ViCA alkalmazás akkor is használható hitelesítésre, ha a felhasználó mobiltelefonról vagy táblagépről veszi igénybe a bank szolgáltatásait.

Az **SMS jelszó** csak egy egyszeri hitelesítési kódot tartalmaz, míg a ViCA a felhasználó privát kulcsával végzi el a megbízások aláírását.

A **QR kóddal** végezhető autentikációs és autorizációs eljárásnál a ViCA használata a felhasználók számára kényelmesebb, és gyorsabban végrehajtható műveletet jelent, mellyel egyben a felhasználói élmény is fokozottabb. A ViCA a megbízások aláírása során lehetőséget biztosít az egyes tranzakciós adatok megmutatására (PSD2 EBA-RTS előírás), ami a QR kód használata esetén nem lehetséges.

Az alkalmazás szabványos és könnyen auditálható eszközökkel és algoritmusokkal dolgozik (RSA, SSL, PBKDF2).

2.1 A ViCA alkalmazás elérhetősége

A ViCA alkalmazást, annak tulajdonosaként a Cardinal Kft. tölti fel az App Store-ba, a Google Play-be valamint a Microsoft Store-ba, azokat saját fejlesztői tanúsítvánnyal aláírva.

A ViCA applikáció az iOS 10+, az Android 4.1+ operációs rendszert futtató telefonokra és tabletekre, a Desktop ViCA a Windows win7 ás win10 operációs környezetekre érhető el. A folyamatosan frissülő verziójú operációs rendszerekre a fejlesztés is folyamatos.

2.2 A ViCA igénybevételének technikai feltételei – felhasználói oldalon

1. **Okostelefon** vagy táblagép használata:
    - Android eszközök: Android 4.1 vagy újabb verziójú operációs rendszer;
    - iOS eszközök (iPhone/iPad/iPod touch): iOS 10.0 vagy újabb verziójú operációs rendszer szükséges.
2. **Desktop** (asztali számítógépen használt) ViCA esetében:
    - Windows win7 vagy win10 verziójú operációs rendszer.
3. A ViCA applikáció – mint hitelesítési eszköz – előzetes banki admin felületen a felhasználóhoz való hozzárendelését követően a bank által SMS-ben küldött ViCA regisztrációs **jelszó fogadása**,
4. Az alkalmazás regisztrációjához, majd a későbbi működéséhez **internet kapcsolat** (mobilinternet, WiFi, illetve vezetékes – Desktop ViCA esetén) azon az eszközön, amin az alkalmazás telepítésre került.

2.3 Az alkalmazás telepítése

A felhasználó az alkalmazást az App Store-on, a Google Play-en illetve a Microsoft Store-on keresztül tudja mobil eszközére vagy Desktop ViCA esetén asztali számítógépére telepíteni.

Az alkalmazás első indításakor a felhasználónak meg kell adnia a ViCA jelszavát. Ez a **ViCA jelszó** védi a ViCA alkalmazást, ismerete nélkül azt nem lehet elindítani. Felépítése minden bankban azonos, a biztonság érdekében a Cardinal Kft. határozza meg a jelszó felépítésének követelményeit (jelszó policy). A jelszó betűk és számjegyek kombinációja, mely minimum 8 és maximum 16 karakter hosszú lehet. A választott jelszó erősségét az applikáció a felhasználói felületen visszajelzi. A ViCA jelszó policy-ja a ViCÁ-t használó bankok saját policy-jai közül a legerősebb, legszigorúbb. Regisztráció után az alkalmazást csak ezzel a jelszóval lehet elindítani.

2.4 Tanúsítvány generálása és regisztrálása

Miután a számlavezető bank az adott felhasználó hitelesítő eszközeként a saját banki Electra Admin felületén a ViCA-t a felhasználóhoz rendelte és a felhasználó a saját eszközének operációs rendszerének megfelelő Store-ból az alkalmazást a készülékére sikeresen telepítette, a regisztráció első lépéseként a felhasználónak regisztrálnia kell a ViCA alkalmazást a kiválasztott bankba. A folyamat során a felhasználó egy privát-publikus kulcspárt generáltat az alkalmazással. Ehhez az alkalmazásban meg kell adnia **Electra csoportkódját** (amennyiben rendelkezik ilyennel), **rövid nevét** (vagy alias-át), valamint **bejelentkezési jelszavát**. Számlavezető bankja ez alapján a ViCA regisztrációhoz előzetesen megadott mobil telefonszámra egy **megerősítő SMS-ben egy OTP kódot küld** a mobil készülékére, melyet a regisztráció képernyőjén az erre

kialakított mezőbe kell visszagépelnie. A megerősítő OTP kód időkorlátos, ez köti össze a felhasználó azonosítóját és a ViCA applikációt (és annak futtató készülékét).

Az alkalmazás ekkor egy standard tanúsítvány-generálási kérést (CSR) küld a szervernek PKCS#10 formában, a szerver pedig a publikus kulcsból a szerver saját titkos kulcsával aláírva elkészít egy tanúsítványt, a ViCA jelszóból képzett PBKDF kódot pedig beregisztrálja a szerverbe. A ViCA által létrehozott privát kulcsok és tanúsítványok egy évig érvényesek, lejáratuk előtt egy hónappal a ViCA alkalmazás automatikusan megújítja a tanúsítványt.

A tanúsítvány regisztrálásának előfeltétele, hogy a számlavezető pénzintézet az adott felhasználó számára a ViCA használatot engedélyezze saját banki Admin programjában az Electra szerveren.

A tanúsítvány kizárólag olyan adatot tartalmaz, melyet a telefonból egyébként is ki lehet nyerni. Nem tartalmaz felhasználó nevet, vagy egyéb szenzitív információt. (A telefon elvesztése vagy eltulajdonítása esetén tehát abból **titkos adatot kinyerni nem lehet**).

Sikeres regisztráció után a privát kulcs titkosított formában mentésre kerül az eszközön. A titkosításhoz használt kulcs egyik fele a telepített alkalmazást használó eszköz paramétereiből áll elő, míg annak másik felét az Electra szerver tárolja, és azt kizárólag a megfelelő ViCA jelszó megadásakor adja át az alkalmazásnak. Az Electra szerver **három sikertelen ViCA jelszó megadása esetén a felhasználót kitiltja**. (Megfelelő /mobil/ eszköz és ViCA jelszó nélkül a privát kulcs kititkosítása nem lehetséges).

A ViCA jelszót a ViCA alkalmazás nem tárolja – kódolt formában sem.

2.5 Alkalmazás indulásakor

Induláskor az alkalmazás bekéri a ViCA jelszót, majd a tanúsítvánnyal és a ViCA jelszóval belép a banki szerverre. Ha a ViCA belépéskor a bankba beküldött adatok helyesek, az Electra szerver visszaküldi a korábban regisztrált privát kulcs kititkosításához szükséges szerverkulcsot. **A ViCA alkalmazás a ViCA jelszót sehol nem tárolja, annak helyességét a banki központ ellenőrzi, tehát a ViCA jelszót szisztematikus próbálkozásokkal nem lehet meghatározni**. Három egymást követő ViCA jelszó tévesztés után a ViCA belépés a banki központban letiltásra kerül. Ezzel egy ezt követő helyes jelszó megadása esetén sem lehetséges a ViCA alkalmazás belépése a szerverre. A ViCA alkalmazás a szerveren tárolt titkosítási kulccsal védi a lokálisan tárolt privát kulcsát. A banki szerver nélkül a lokálisan titkosított privát kulcs nem visszafejthető, ugyanakkor a banki szerveren a titkosított privát kulcs nem létezik.

Mivel **az applikáció multibankos**, ezért a jelszavak ellenőrzése és a rontott jelszavak banki nyilvántartása egy beépített algoritmus szerint a beregisztrált bankok használati gyakorisága szerinti sorrendben történik.

2.6 Több felhasználó beregisztrálása

Bizonyos bankokban lehetőség van arra, hogy egy felhasználó több banki felhasználó nevében is beregisztráljon. Erre jellemzően akkor van szükség, ha egy természetes személy több ügyfélnél több banki felhasználóként jelenik meg. Fontos, hogy ebben az esetben a „több banki felhasználó" ugyanazt a természetes személyt takarja, és erről a bank meggyőződjön, és a felhasználót azonosítsa.

Erre a Regisztráció menüpontban van lehetőség. Az összes felhasználó regisztrációja a fentiekben ismertetett módon történik, annyi különbséggel, hogy az első regisztrációt követő további regisztrációk során nem készül új kulcspár és tanúsítvány: **az aláírás ugyanazzal a tanúsítvánnyal történik.**

2.7 Tanúsítvány használata bejelentkezéskor (autentikáció)

Az alkalmazás az Internet Bankingbe, az Electra Ügyfélprogramba, valamint a Mobil Banking és Electra MobilApp rendszerekbe történő belépéshez használható a felhasználó kilétének biztonságos autentikációjához.

A banki rendszerekbe való belépési folyamatban a felhasználó azonosítása az adott felületen megadott felhasználói azonosító segítségével kezdeményezhető. Android, iOS és Windows 10 applikációk használatakor a ViCA-t futtató eszköz egy push üzenetet kap a szervertől, melyben a felhasználó tájékoztatást kap arról, hogy a belépéshez a ViCA applikáció elindítására és használatára van szükség. A belépést a ViCA alkalmazásban kell jóváhagyni. A jóváhagyás után a belépési folyamat automatikusan folytatódik az érintett Electra kliensen. Az alkalmazás a privát kulcs és a hozzá tartozó tanúsítvány segítségével elvégzi az Electra kliensre való bejelentkezés befejezéséhez szükséges műveleteket, majd a felület automatikusan tovább lépteti a felhasználót az Ügyfélprogram bejelentkezés utáni, illetve az Internet Banking áttekintő oldalára.

2.8 Tanúsítvány használata aláíráskor (autorizáció)

Az Electra Ügyfélprogramban, az Internet-, illetve Molbil Bankingben, valamint a MobilAppban a felhasználó kiválasztja az általa aláírni kívánt csomagokat (azonnali beküldés esetén sikeresen elvégezte a megbízás hibátlan rögzítését). Az adott Electra kliens felület jelzi a felhasználónak, hogy indítsa el a mobil eszközön a ViCA alkalmazást és válassza ki a megfelelő funkciót. (Erről az Android, iOS és Windows 10 operációs rendszeren futtatott applikációk push üzenetet is kapnak).

Az alkalmazásban **megjelennek az aláíróhoz tartozó információk**: csomagnevek, célszámlák és az egyes megbízások összegei, az aláíró felhasználó neve és az aláírás időpontja. A ViCA jelszó megadását követő jóváhagyás után a csomagok aláírása elkészül. Az Electra kliens felület automatikusan tovább lép a nyugtázó képernyőre (aláírások elkészültek) illetve azonnali beküldés esetében a megbízást egyből be is küldi a bankba.

A ViCA alkalmazásban a felhasználónak **lehetősége van a kliensből**

kezdeményezett aláírás elutasítására. Ilyenkor a kliens felület figyelmeztető üzenetet jelenít meg az elutasításról, és az aláírásra kijelölt megbízási csomagok változatlanok maradnak.

Bizonyos bankokban – kifejezett banki kérésére – biztonsági okokból az applikáció **minden egyes aláírást közvetlenül megelőzve bekéri a ViCA jelszót** is, mely a banki központba való felküldéskor ellenőrzésre kerül.

2.9 Biometrikus azonosítás

Az Android és az iOS operációs rendszert futtató applikációkban lehetőség van a regisztrációt követően biometrikus azonosításra váltani. Ezt választva annak beállítása után a ViCA applikáció indításakor nem szükséges a ViCA jelszó megadása, helyette az **adott eszköz és operációs rendszer által biztosított biztonságos biometrikus azonosítást lehet igénybe venni**. Ez a kényelmi funkció az Androidos verzió esetén applikáción belül ki- illetve bekapcsolható, iOS esetén pedig az ViCA első futásakor illetve jelszócsere esetén lehet a biometrikus azonosítást bekapcsolni.

A szolgáltatás igénybe vételéhez szükséges, hogy a mobil eszköz rendelkezzen ujjlenyomat olvasási funkcióval.

2.10 Jelszó módosítás

A ViCA jelszó módosítására **az applikációban külön menüpont szolgál**. A jelszócsere csak akkor végezhető el, ha minden beregisztrált banki szerver elérhető és támogatja a jelszócsere funkciót, hiszen a megváltoztatott jelszavát az összes bankban érvényesíteni kell. Amennyiben a csere valamennyi érintett banki szerveren sikerült, a felhasználó erről tájékoztatást kap, és ezt követően kizárólag új ViCA jelszavával tudja az applikációját használni.

2.11 Kapcsolódási sorrend figyelése

A ViCA alkalmazás figyeli, hogy a beregisztrált bankok közül a felhasználó melyiket használja a leggyakrabban, azaz melyiktől jön a legtöbb bejelentkezési és aláírási üzenet. Az alkalmazás **az üzenetek számától függően rendezi sorrendbe a bankokat, és ahhoz a bankhoz kapcsolódik elsőként, amelyet a felhasználó a leggyakrabban használ.**

Mivel a legelsőként kapcsolódott bank végzi el a ViCA jelszó ellenőrzését, ezzel elkerülhető, hogy jelszórontás esetén egy ritkán használt bankban kerüljön kitiltásra a felhasználó, ahol – a ritka használat miatt – a felhasználónak problémát okozhat a feloldáshoz kapcsolódó ügyintézés.

A beérkezett üzenetek számától az alkalmazás hetente egyszer, a heti első használat alkalmával számolja újra a bankok sorrendjét.

2.12 ViCA push üzenetküldő szolgáltatás

A VMS banki környezetbe való telepítésével lehetővé válik a ViCA alkalmazás további szolgáltatásának elérése: a banki feldolgozó- és kommunikációs rendszerekből indított különböző típusú és tartalmú üzenetek küldése és azok fogadása és kezelése az ügyfelek mobil eszközein. A szolgáltatás **költségtakarékos**, hisz a bankok ingyenesen tudják az egyes felhasználókra vonatkozó célzott üzeneteiket továbbítani.

Ezek az alábbi értesítések lehetnek:

- Adott számlák egyenlege,
- Tranzakciós értesítések,
- Nem teljesült ill. visszautasított megbízások,
- Beérkezett fizetési kérelem üzenetek,
- Új, aláírásra váró megbízáscsomagok elérése,
- Aktuális hiteltörlesztések,
- Fizetési határidők figyelmeztetései,
- Kártyaőr és számlaőr szolgáltatások,
- Banki hírek,
- Személyre szabott banki termékajánlatok, promóciós kampányok, illetve
- Egyéb üzenetek.

Az alkalmazás a VMS közbeiktatása miatt nemcsak az Electra rendszerből, hanem megfelelő API-n keresztül **más banki rendszerekből is képes üzenetek továbbítására**.

Abban az esetben, ha a ViCA alkalmazás a felhasználó mobil eszközén nincs megnyitva, a telefon egy push üzenetet jelenít meg a felhasználó eszközén a ViCA applikációra küldött üzenet tényéről. Fontos, hogy maga **a push értesítő személyes vagy üzleti adatot nem tartalmaz.**

A mobil alkalmazás következő megnyitásakor a felhasználó ViCA alkalmazása kapcsolódik a VMS-hez, ahonnan a konkrét üzenet, annak már teljes tartalmával együtt, **SSL-lel védett csatornán** keresztül érkezik meg a felhasználó mobil eszközére.

A beérkezett üzenetek „tárgyuk” szerint jól átlátható, táblázatos formában kerülnek megjelenítésre az érintőképernyőn. Ha a „tárgy” mezőben küldött információn túl a bank további üzenettartalomat is elhelyezett, úgy a „tárgyra” kattintva az üzenet teljes tartalmát a ViCA egy **view-ban jeleníti meg**. Amennyiben a felhasználó az elolvasott üzenetet bezárja, úgy visszalép a push értesítések összefoglaló táblázatához.

A ViCA üzenetküldő szolgáltatása nyelvfüggő, azaz, ha a „tárgy” több nyelven is elküldésre került, úgy a ViCA felismeri azt és az alkalmazás beállított nyelve szerinti tartalmat mutatja csak a felhasználó részére.

A bank által **kiküldött ViCA üzenetekről a rendszer statisztikát is készít**, melyet a banki WebAdmin felületen a kívánt csoportosítás szerint lehet lekérdezni. (ViCA üzenet tárgya és tartalma, az üzenet státusza, a címzettnek való kézbesítés időpontja, az SMS fallback ideje, külső ID).

A kínált megoldás opcionálisan lehetőséget biztosít **fallback mechanizmusokra** is. Így a felhasználó SMS-ben is megkaphatja az üzenetet, ha azt meghatározott ideig nem töltötte le a ViCA alkalmazásban.

Opcionálisan beállítható egy **„SMS timer”**, melyben meghatározott idő eltelte után a VMS egy paraméterként megadott SMS tartalom értéket küld meg a bankba regisztrált felhasználó mobil készülékére.

A **„Message timer”** beállításával időben korlátozható az üzenet lejárata is, ameddig a kiküldött ViCA üzenet a felhasználó telefonján letölthető.

A **„Külső ID”** a bank által használt saját azonosító, ami a bank számára az üzenetek visszapárosítását teszi lehetővé (nem jelenik meg az App felületén).

2.12.1 Electra WebAdmin funkció ViCA üzenetek lekérdezésére

Az Electra WebAdmin felületén **a kiküldött ViCA üzenetek lekérdezése** a bank számára **külön funkcióként érhető el** az alábbi információkat illetően:

- ViCA üzenet tárgya, tartalma,
- Üzenet státusza,
- Milyen időpontban jutott el a címzetthez,
- SMS fallback ideje,
- Külső ID (a banki üzenetek visszapárosítását lehetővé tevő banki saját azonosító).

A lekérdezett tartalom a felületről exportálható.

3. A ViCA alkalmazás architektúrája

A ViCA alkalmazás egy **független, SSL titkosítással védett TCP/IP csatornát nyit az Electra szerverre, illetve a ViCA Mikro Szerverre**. Az Electra szerver, illetve a ViCA Mikro Szerver IP címe az alkalmazásba van bekódolva, mely a fejlesztő kulcsával került aláírásra, így az az alkalmazást külső manipulálás ellen az operációs rendszer védi. A ViCA és az Electra szerver, illetve a ViCA Mikro Szerver között egyedi kommunikációs protokoll van (tehát nem HTTPS), így a protokoll ismerete nélkül azt támadni nem lehet, a "szokásos" HTTP protokoll támadások hatástalanok.

A használat során ez azt jelenti, hogy az aláíráskor az **Electra csatornától teljesen független csatorna épül fel** a ViCA alkalmazás és az Electra szerver, illetve ViCA Mikro Szerver között. Az aláíráshoz szükséges autentikációs adatokat az Electra

szerver, illetve a ViCA Mikro Szerver ezen a külön csatornán küldi el a ViCA alkalmazásnak.

4. ViCA Mikro Szerver (VMS)

A ViCA Mikro Szerver egy olyan önállóan működtethető szerver, mely a ViCA alkalmazással kapcsolatos műveleteket kezeli. Saját adatbázist kezel, melyben nyilvántartja az aktuálisan beregisztrált, valamint regisztrációra váró felhasználókat.

A VMS az iOS, az Android, valamint a Windows win7 és win10 operációs platformon futó ViCA alkalmazásokat szolgálja ki. Az ezeket a platformokat használó eszközökre célzott push üzenetek küldhetőek különböző banki háttérrendszerekből az egyes felhasználók számára.

A ViCA Mikro Szerver banki környezetben való implementálásával az Electra csatornák felhasználóinak kiszolgálásán kívül, **WebService hívásokon keresztül** lehetőséget biztosít arra is, hogy a bank más **külső rendszerei is igénybe vegyék** a ViCA szolgáltatásait. Tehát a bank akár az Electra rendszert használó felhasználókat, akár az **Electrától teljesen független felhasználói kört is kezelheti** ViCA alkalmazással. Az egyes banki ügyfélköröket a VMS egymástól elkülönítetten kezeli.

Lehetőség van az Electra vonatkozású felhasználók bizonyos irányú műveleteinek harmadik félnek történő kiajánlására is (pl. a bank dedikált üzenetet tud küldeni csak az Electra csatornákat használó ViCA felhasználóknak).

A VMS technikailag kétfajta üzemmódban futtatható a banki környezetben: önállóan illetve beágyazott módon.

A beágyazott esetben az Electra szerver részét képezi a VMS, amely így együtt indul és áll le az Electra szerverrel, ilyenkor nincs mód WebService elérésre, tehát csak az Electra szerver rendelkezik a ViCA felhasználók felett (egyéb banki feldolgozó rendszerek nem).

4.1 ViCA Mikro Szerver WebService API

A ViCA Mikro Szerver (VMS) WebService segítségével más banki rendszerek számára is lehetőség nyílik arra, hogy üzeneteket juttassanak el a felhasználók számára a ViCA alkalmazáson keresztül.

Az **üzenetküldés** mellett, a külső rendszerek a ViCA Mikro Szerver szolgáltatásán keresztül igénybe vehetik a ViCA **autentikációt** is. Ha egy banki rendszernek **erős ügyfélautentikáció**ra van szüksége, ezen az API-n keresztül tudja kezdeményezni és menedzselni a ViCA autentikáció folyamatát.

Az **API által biztosított funkciók**:

- ViCA push értesítések és üzenetküldés,
- Felhasználói autentikáció indítása,
- Felhasználói megbízások aláírásának ellenőrzése,

- ViCA regisztráció engedélyezése,
- ViCA regisztráció tiltása,
- ViCA regisztrációk lekérése,
- üzenetek lekérése, szűrése.

5. Referencia lista

Jelenleg az alábbi pénzintézetek használják a ViCA autentikációs eszközt: