Cardinal Számítástechnikai Kft.

Kétcsatornás autentikáció

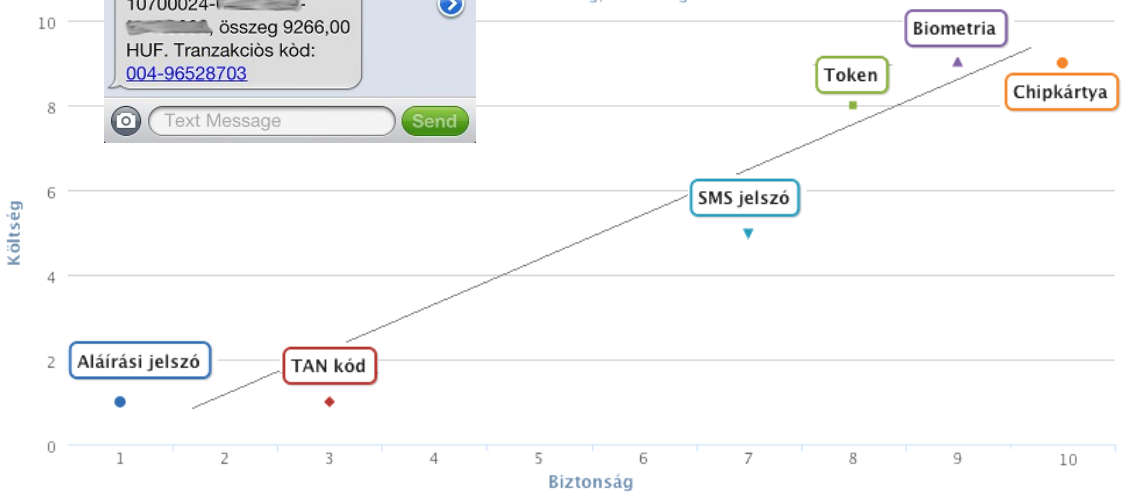
Az internet banking rendszerek biztonságának aktuális kérdései

Gyimesi István, fejlesztési vezető, Cardinal Kft.

Az előző részek tartalmából...

E-Banking Summit 2012, Cardinal Kft.:
Felhasználók azonosítása elektronikus banki rendszerekben

- Jelszavas azonosítás
- TAN kód
- Token
- Biometrikus azonosítás
- SMS jelszó
- Chipkártya



Az előző részek tartalmából...

E-Banking Summit 2012, Cardinal Kft.:
Felhasználók azonosítása elektronikus banki rendszerekben

...

2013...

A biztonság kérdése aktuálisabb, mint valaha!

2013...

- Eurograbber: 36 millió eurós kár (2012. december)
  (http://www.informationweek.com/security/attacks/zeus-botnet-eurograbber-steals-47-millio/240143837)
- Magyarország: Százmilliós nagyságrendű kár (forintban, 2013. február)
  (http://www.penzcentrum.hu/tech/veszelyben_a_magyar_netbankolok_szazmilliokat_nyultak_le.1035381.html)

Eurograbber

(www.checkpoint.com/products/.../Eurograbber_White_Paper.pdf)

- vírustámadás a felhasználó gépe ellen
- a gép botnetbe szervezése
- operációs rendszer megfertőzése, weboldalak meghamisítása
- „biztonság fejlesztése” címszó alatt telefon típusának, telefonszám bekérése
- támadó SMS küldése a telefonra
- SMS-ben lévő linkre kattintva vírus telepítése a telefonra IS!

Eurograbber

(www.checkpoint.com/products/.../Eurograbber_White_Paper.pdf)

Működés:

- Felhasználó bejelentkezik a NetBankba
- A vírus aktiválja magát
- A támadó indít egy tranzakciót
- A tranzakciós SMS-t lenyúlja a mobilra telepített vírus
- A támadó ellopta a felhasználó pénzét anélkül, hogy a felhasználó bármit észrevett volna.

Magyarország

- vírustámadás a felhasználó gépe ellen
- a gép botnetbe szervezése
- operációs rendszer megfertőzése, weboldalak meghamisítása
- a beszúrt oldalak különböző indokokra hivatkozva (megerősített bejelentkezés, rontott belépési kód, karbantartás) új token kód, SMS kód bekérése

Magyarország

Működése

- A felhasználó behívja a bejelentkező oldalt
- Az oldalt a vírus megmódosítja, elküldi a támadónak a megadott azonosító adatokat
- (A felhasználó felülete ezután ténylegesen nincs kapcsolatban a bank szervereivel!)
- A támadó bejelentkezik és tranzakció indítását kezdeményezi
- A vírus által beszúrt oldal még egy token kódot, vagy az SMS-ben kiküldött kódot kéri be
- Ez is elkerül a támadóhoz, aki el tudja indítani az utalást, a felhasználó tudta nélkül ellopja annak pénzét.

Új jellemzői a támadásnak

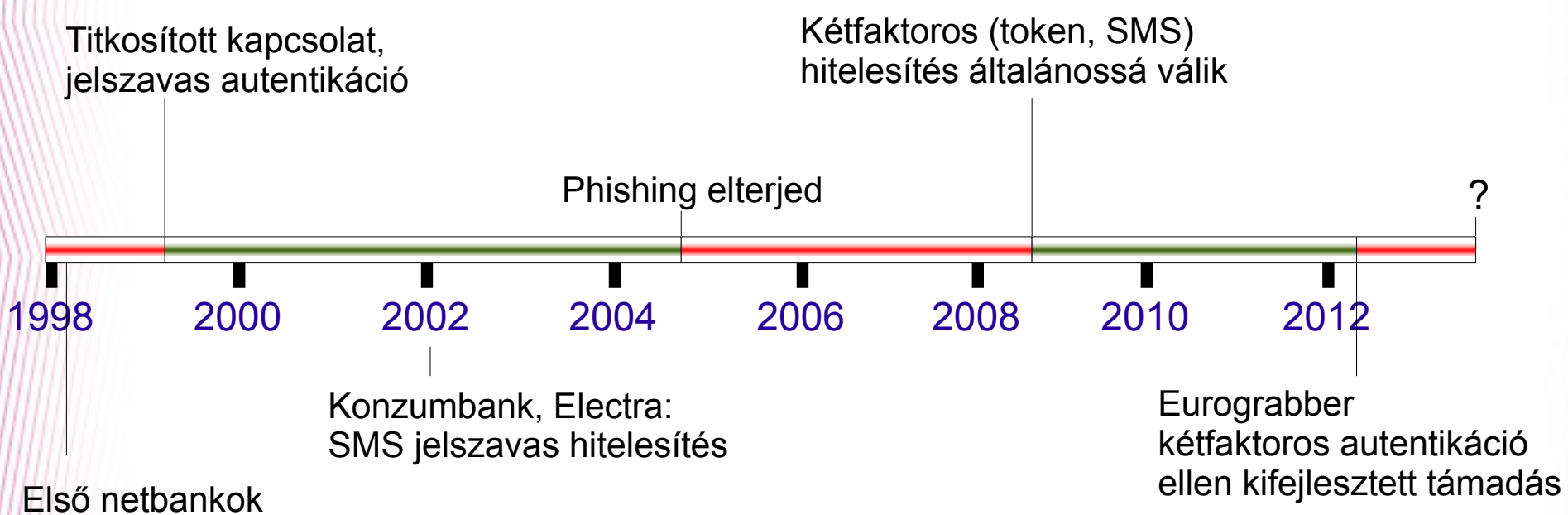
- A böngészőprogramokat támadják meg
- Kétfaktoros autentikáció hatástalanítása
- Adott banki rendszerre szabott támadás (nem csak a felület kinézetében, hanem működési módjában!)
- Aktívan módosítják a támadás módját:
  - megkeressük a támadás gyenge pontját
  - módosítjuk a felületet, hogy ennél fogva hatástalanná tegyük a támadást
  - pár nap múlva reagálnak a támadók, módosítják a támadást

Bank vs. Támadók

- A banknak követnie kell az elektronikus szolgáltatásokra vonatkozó belső szabályzataikat
- A támadónak nincsenek szabályzatai

Mivel a támadónak teljes kontrollja van a felhasználó gépe felett, ezért távolról (a bankból) nem lehet végleges megoldást adni!

Miért most?



: Bankbiztonság jár előrébb

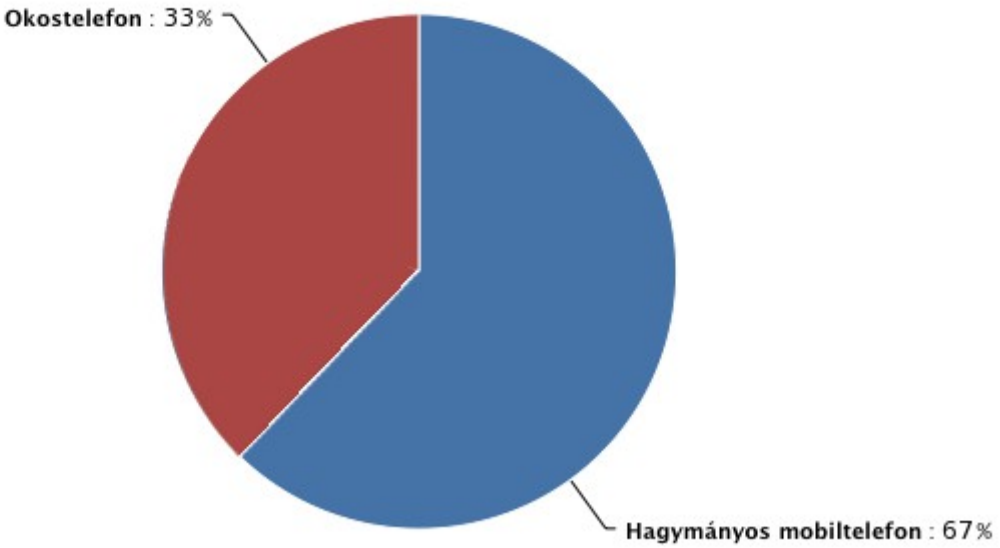
: Támadók járnak előrébb

Mi lehet a megoldás?

- A kétfaktoros autentikáció már nem nyújt elég biztonságot.
- Chipkártya?
  - Telefonokon, tableteken nem használhatók.
  - Amint általánosan elterjed a chipkártyás hitelesítés, azt fogják támadni.
  - Ha az ügyfél gépe felett egy vírus segítségével a támadó teljesen átveszi az irányítást, akkor abban sem lehetek biztos, hogy a chipkártyás hitelesítés tényleg az én tranzakciómat fogja aláírni.

Mit hoz a jövő?

Okostelefonok piaci részesedése Magyarországon (2012. december)



- Ez kb. hárommillió darab okostelefont jelent
- 2011. novemberéhez képest egymilliós növekedés
- Az elektronikus banki szolgáltatások használók körében ez az arány még jobb

A mi megoldásunk:

Kétcsatornás autentikáció: ViCA

(Virtuális Chipkártya Alkalmazás)

ViCA

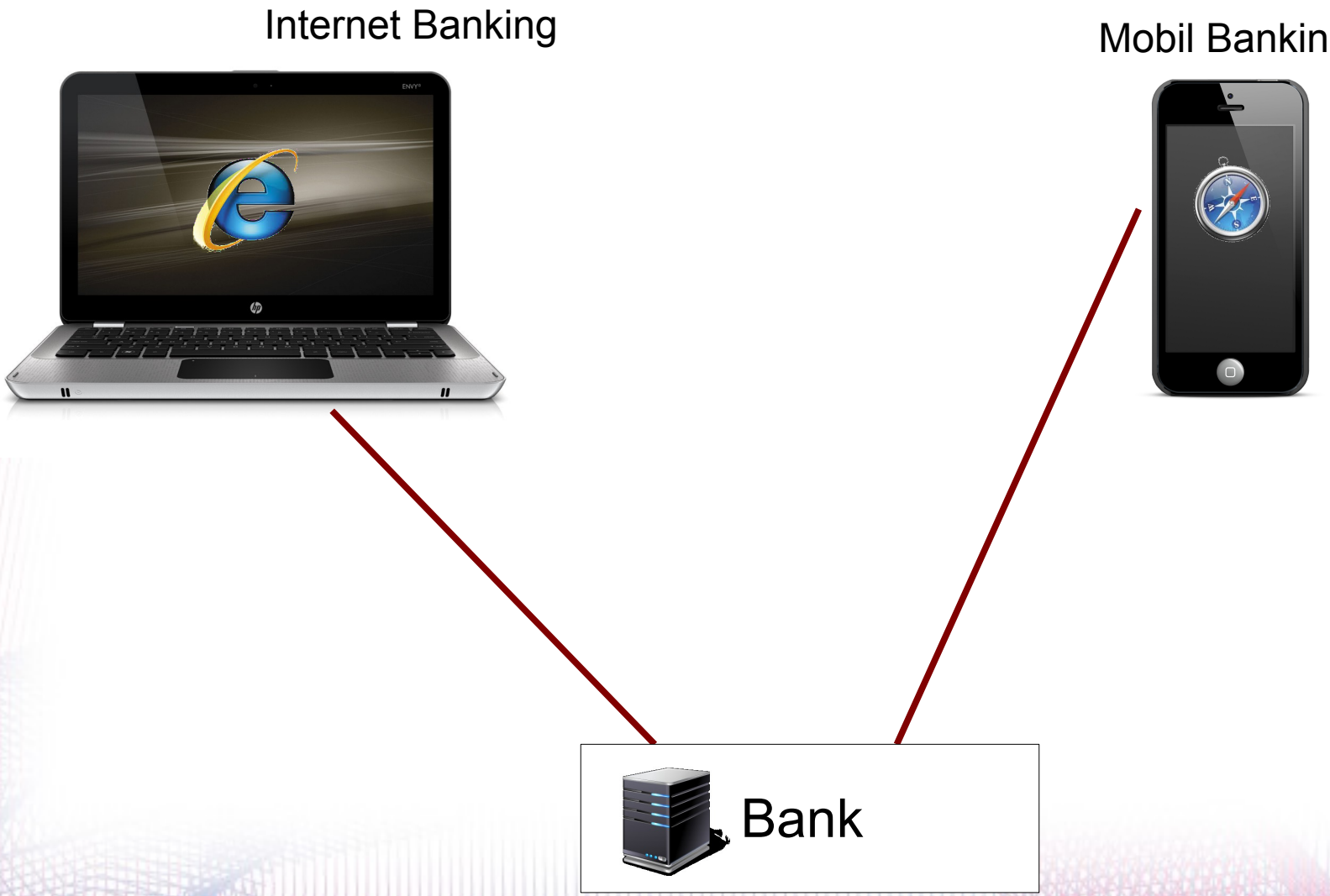
Okostelefon alkalmazás Internet Bankinghez, Mobil bankinghez és vastag klienshez:

- Felhasználók azonosítására
- Megbízások, csomagok aláírására
- Phishing, pharming és Eurograbber-szerű támadás elleni védelemre

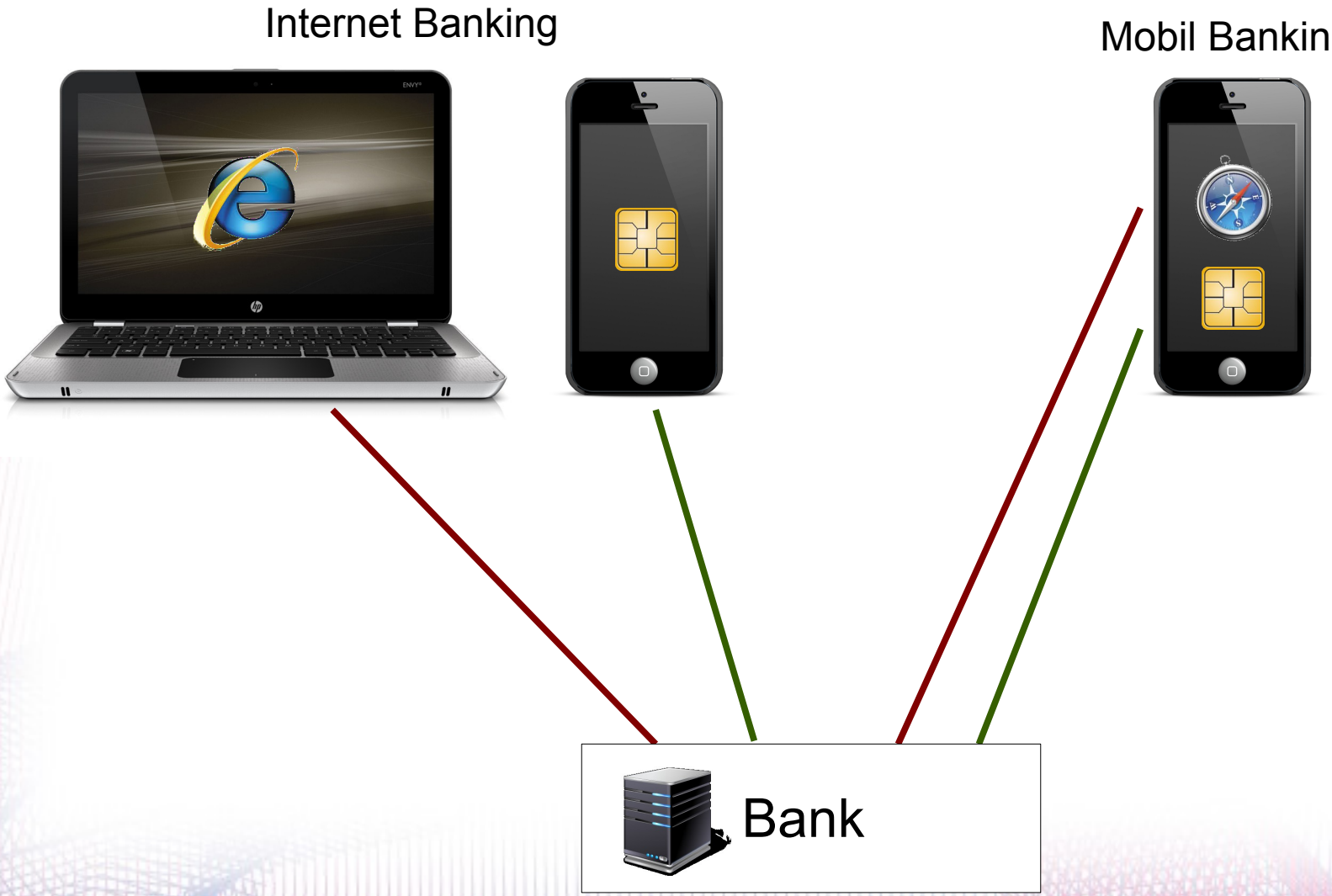
ViCA

- “Virtuális chipkártya”: Személyes hitelesítő eszköz, be kell regisztrálni a bank elektronikus banki rendszerére
- Iparági szabványoknak megfelelően, biztonságos módon tárol egy kulcsot.
- Ezzel a kulccsal azonosítja magát a felhasználó, ezzel írja alá digitálisan a tranzakcióit.
- Alkalmazás, amit mindig nehezebb törni (a vastag kliensek nem is érintettek a mostani támadásokban)
- Zárt kommunikációs protokoll
- A kulcs nem kerül ki az alkalmazásból

Mit jelent, hogy kétcsatornás?



Mit jelent, hogy kétcsatornás?



Mit jelent, hogy kétcsatornás?

- Digitálisan aláírt, a böngészőprogramtól független alkalmazás
- Saját, biztonságos kapcsolatot épít ki a bank szervereivel
- Ezt a kapcsolatot nem lehet eltéríteni, lehallgatni
- A böngésző és a bank közötti, fertőzött kapcsolaton keresztül semmilyen titok nem utazik

- Az alkalmazás sokkal több információt tud megmutatni az aktuálisan végrehajtott műveletekről, mint ami egy SMS-be belefér.
- „Hab a tortán”: nincs SMS költség!

Cardinal Számítástechnikai Kft.

ViCA – chipkártya összehasonlítás

	Chipkártya	ViCA
Fizikai eszköz	Plasztikkártya	Okostelefon
Hozzáférés	PIN-kód	ViCA jelszó
Funkciók	Bejelentkezés és aláírás	Bejelentkezés,aláírás és biztonságos üzenetküldés
Aláírás	RSA kulcspár	RSA kulcspár
Bejelentkezés	RSA kulcspár	RSA kulcspár
Üzenetek kezelése	-	ViCA jelszóval védve
Hozzáférés a privát kulcshoz	Hardveres védelem	Online, banki szerver védelem
Hordozhatóság	Csatlakoztatni kell a számítógéphez, meghajtókat kell telepíteni	Mobil, független eszköz
Költségek	Fizikai eszközöket (kártyaolvasó, kártya) kell vásárolni	A ViCA alkalmazás ingyenes

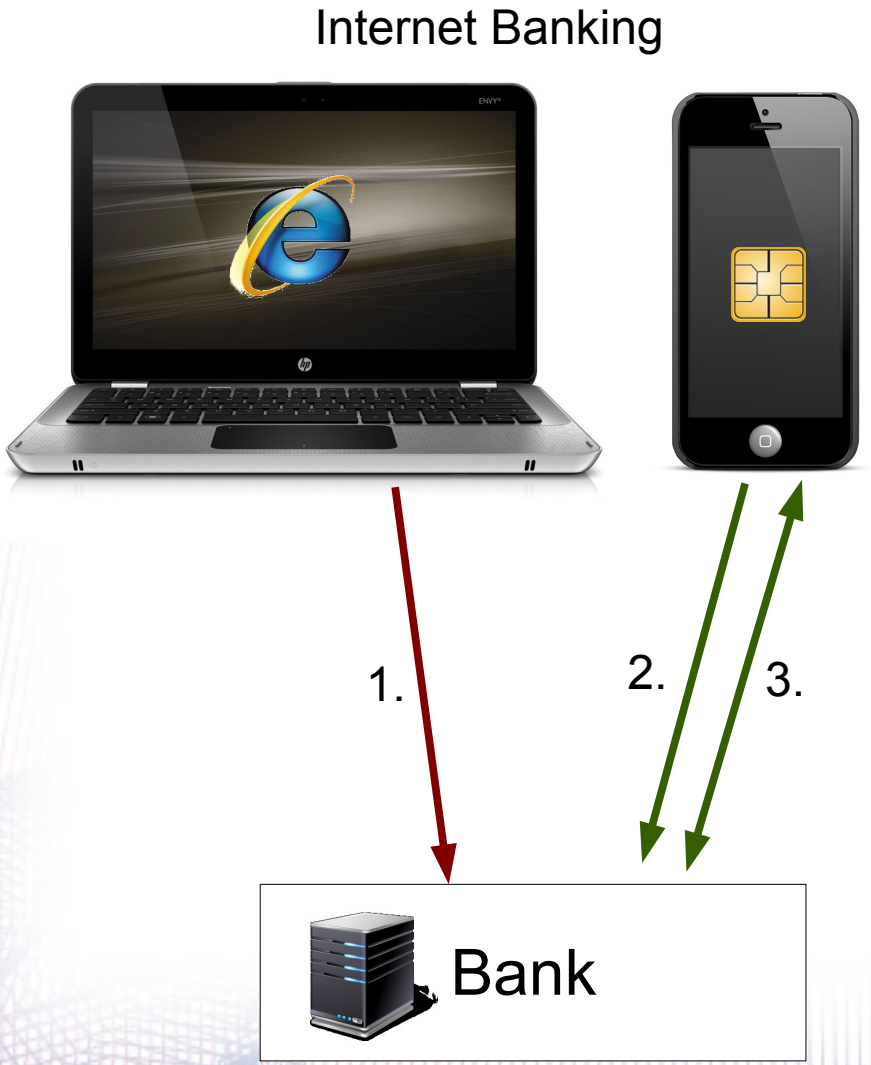
ViCA - bejelentkezés

1. A felhasználó megadja az internet (vagy mobil) banking felületen a felhasználó azonosítóját.

ViCA - bejelentkezés

1. A felhasználó megadja az internet (vagy mobil) banking felületen a felhasználó azonosítóját.
2. Elindítja a ViCA alkalmazást, ami kiépíti saját biztonságos kapcsolatát a bankkal.

ViCA - bejelentkezés



1. A felhasználó megadja az internet (vagy mobil) banking felületen a felhasználó azonosítóját.
2. Elindítja a ViCA alkalmazást, ami kiépíti saját biztonságos kapcsolatát a bankkal.
3. Megtörténik a felhasználó autentikációja ezen a csatornán keresztül.

ViCA - bejelentkezés

Internet Banking

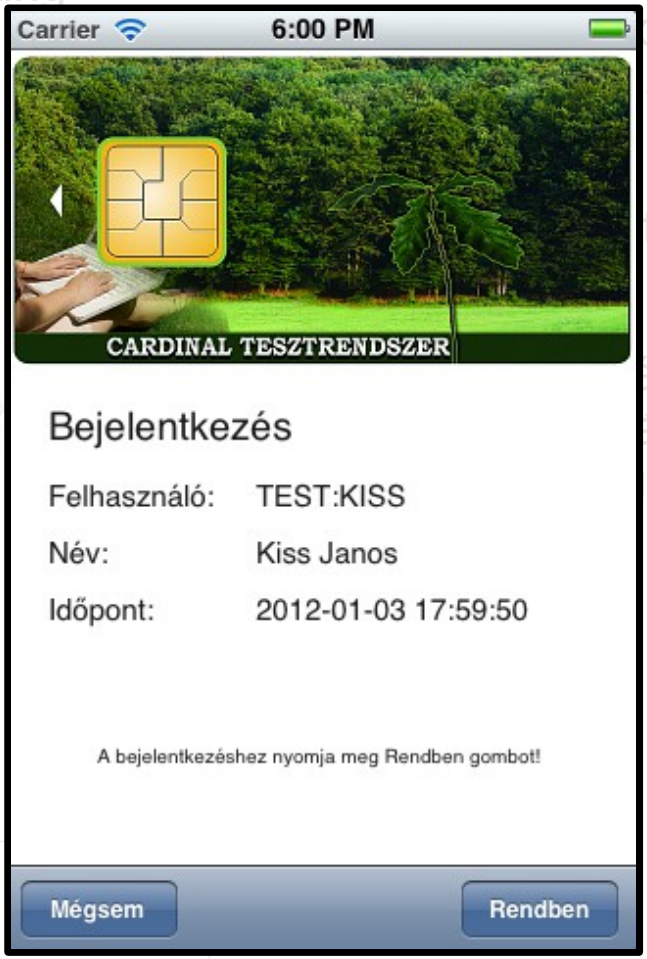
1. A felhasználó megadja az internet
obil) banking felületen a
áló azonosítóját.

a ViCA alkalmazást, ami kiépíti
tonságos kapcsolatát a

ènik a felhasználó
ációja ezen a csatornán
l.

1.

Bank



ViCA - bejelentkezés

1. A felhasználó megadja az internet (vagy mobil) banking felületen a felhasználó azonosítóját.
2. Elindítja a ViCA alkalmazást, ami kiépíti saját biztonságos kapcsolatát a bankkal.
3. Megtörténik a felhasználó autentikációja ezen a csatornán keresztül.
4. Elindul az internet banking munkafolyamat.

ViCA - aláírás

1. A felhasználó berögzíti a tranzakciót.

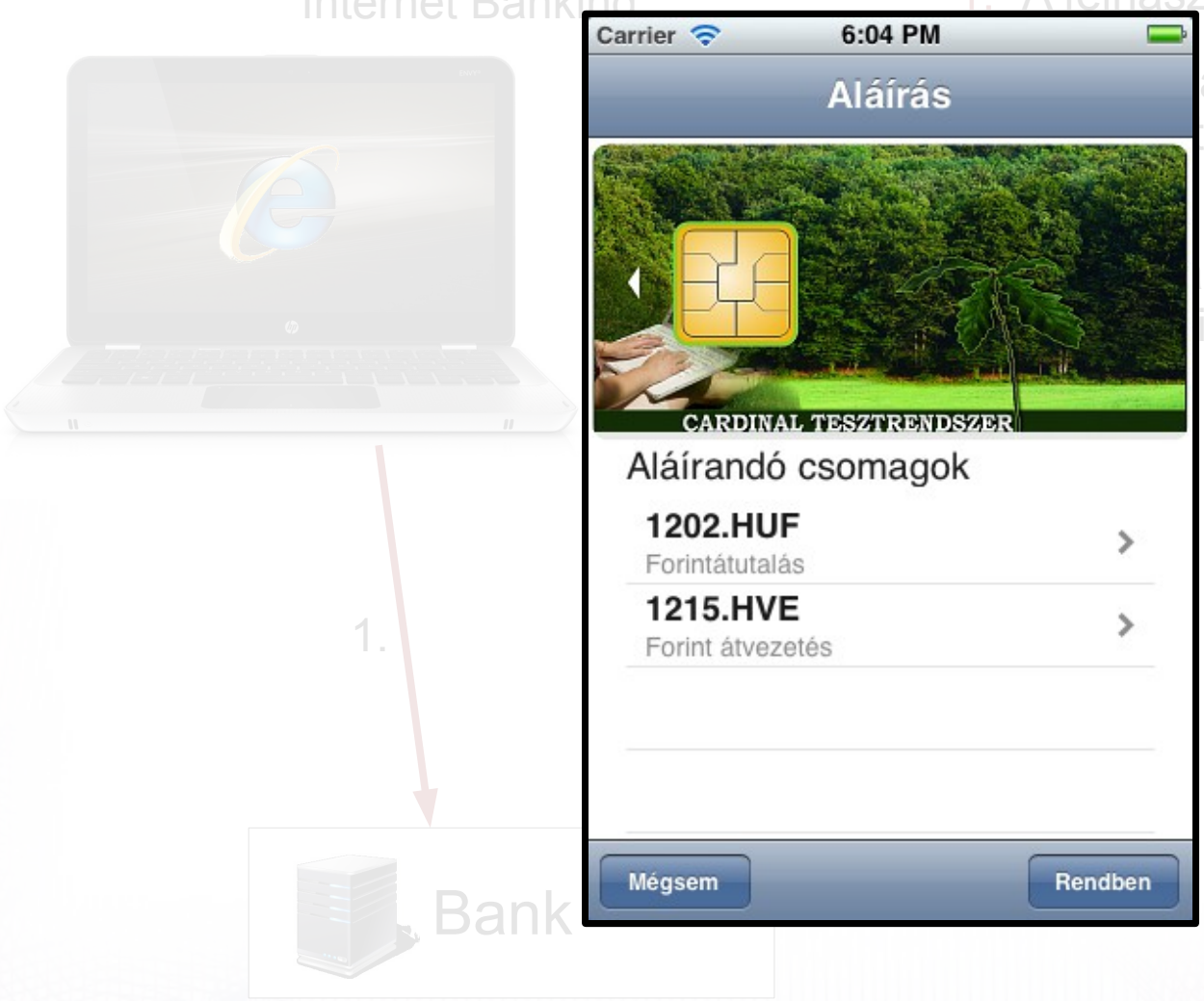
ViCA - aláírás

1. A felhasználó berögzíti a tranzakciót.
2. Elindítja a ViCA alkalmazást, ami kiépíti saját biztonságos kapcsolatát a bankkal.

ViCA - aláírás

1. A felhasználó berögzíti a tranzakciót.
2. Elindítja a ViCA alkalmazást, ami kiépíti saját biztonságos kapcsolatát a bankkal.
3. A ViCA alkalmazás megmutatja a tranzakció adatait (számlaszám, összeg)

ViCA - aláírás



ViCA - aláírás

1. A felhasználó berögzíti a tranzakciót.
2. Elindítja a ViCA alkalmazást, ami kiépíti saját biztonságos kapcsolatát a bankkal.
3. A ViCA alkalmazás megmutatja a tranzakció adatait (számlaszám, összeg)
4. A felhasználó jóváhagyása után a ViCA elkészíti a tranzakció digitális aláírását.
5. A tranzakció elküldhetővé válik az internet bankingben.

Összefoglalva

- Visszakerül az előny a bankokhoz/fejlesztőkhöz
- Gyors választ tudunk adni a mostani támadásokra
- Költséghatékony megoldás
- A technológia levédése folyamatban van
- Jóval rugalmasabb, felhasználóbarátabb és költséghatékonyabb a chipkártyánál
- Önálló szolgáltatásként is megjelenhet

Kétcsatornás autentikáció

Köszönöm a figyelmet