

Bezpečnosť elektronického bankovníctva v praxi

Uverejnenie článku Bezpečnosť vašich on line peňazí alebo Doba sociálneho inžinierstva je späť v PCR č. 4/2001 vyvolalo množstvo reakcií a otázok. V nadväznosti na uvedený článok sa v tomto príspevku bližšie oboznámime s problematikou bezpečnosti elektronického bankovníctva (ďalej EB) a pozrieme sa na bezpečnosť EB v desiatich bankách na Slovensku.

Nie je nijaký dôvod na to, aby sme sa v súvislosti s nedávnym útokom na Internet banking Tatra banky, prípadne inými aktivitami rôznych hackerov vrátili späť k papierovej výmene informácií. Dnes už totiž existujú technológie a riešenia, ktoré umožňujú dosahovať vysokú bezpečnosť a intimitu elektronického výmeny informácií – dokonca vyššiu ako v klasickom papierovom svete. Spomínaný útok je iba výzvou na nevyhnutnú pozornosť a náležitú osvetu pri využívaní progresívnych služieb elektronického bankovníctva.

Každý informačný, resp. komunikačný systém by mal byť chránený v prvom rade ako celok. Mali by mať k nemu prístup iba oprávnené osoby (používatelia), malo by byť možné diferencovať práva rôznych používateľov pri práci s týmto systémom, mal by byť jednoznačne identifikovateľný autor informácie a informácia vymedzená medzi systémom a používateľom by mala byť chránená z hľadiska zachovania jej dôveryhodnosti a integrity. Napokon by mala existovať možnosť riešiť sporné situácie. Pod pojmom sporná situácia sa myslí stav, keď jedna zo zúčastnených strán tvrdí niečo iné ako druhá strana. Napríklad klient bude tvrdiť, že banke neposlal daný platobný príkaz (popretie autorstva, resp. odoslania informácie), alebo bude tvrdiť, že banke síce príkaz poslal, ale uviedol iný cieľový účet, resp. inú sumu (narušenie integrity správy), prípadne banka bude tvrdiť, že daný príkaz od klienta vôbec nedostala (popretie príjmu informácie). Podobné sporné situácie vznikajú všeobecne, preto je potrebné, aby systém EB umožňoval jeho auditovateľnosť v prípade sporu a poskytoval dostatočný dôkazový materiál pre obe strany.

V mnohých prípadoch je dôležitá istota o tom, kto je autorom danej informácie. V klasickom papierovom svete na to slúži podpis, pečiatka, prípadne overenie podpisu notárom. V elektronickom svete by túto požiadavku mal zaručiť elektronický podpis.

Kontrola integrity informácie umožňuje odhaliť akúkoľvek zmenu informácie na ceste od jej autora až po jej spracovanie v danom systéme. Implementácia takejto kontroly do systému EB umožňuje detegovať neúmyselnú zmenu informácie počas jej prenosu, úmyselnú zmenu informácie treťou stranou, ale aj prípadnú zmenu informácie po jej prenose, napr. záškodníkom z vnútra druhej strany.

Elektronické bankovníctvo a jednotlivé jeho formy (distribučné kanály) – terminológia

S ohľadom na nejednoznačnosť názvov distribučných kanálov (foriem EB) v jednotlivých bankách uvádzame kategorizáciu distribučných kanálov EB a ich stručnú charakteristiku, používanú v tomto článku:

HB – Home banking: realizácia platobného styku prostredníctvom špeciálnej klientskej softvérovej aplikácie, ktorá dokáže komunikovať so zodpovedajúcim systémom na bankovej strane. Komunikácia s bankou môže prebiehať cez jednotnú telefónnu sieť (JTS), GSM sieť, Verejnú dátovú sieť (VDS), internet a pod.:

- **HB – klasický Home banking:** aplikácia pre osobný počítač (lokálna stanica, LAN, WAN),
- **MoB – Mobil banking:** aplikácia pre zariadenie PDA (osobný elektronický organizér).
- **IB – Internet banking:** realizácia platobného styku prostredníctvom bežného prehliadača stránok na internete. Komunikácia s bankou prebieha

v súlade so štandardnými protokolmi (HTTP, HTTPS, HTML, WAP, WTLS...):

- **IB – klasický Internet banking** prostredníctvom bežného WWW prehliadača,
- **WB – WAP banking** prostredníctvom WAP prehliadača na telefóne GSM.

TB – Telefón banking: realizácia platobného styku prostredníctvom bežného telefónneho prístroja (často je nutná tónová voľba DTMF), pričom klient dostáva bankové informácie v hlasovej forme:

- **IVR – interaktívny hlasový odpovedač:** komunikácia s automatom,
- **CC – Call Centrum:** komunikácia s operátorom Call Centra.

MeB – Message banking: realizácia platobného styku prostredníctvom správ určitého typu. Reakcia na tieto správy nemusí byť okamžitá ako v predchádzajúcich prípadoch. Ide o správy:

- SMS,
- e-mail,
- fax.

dzajúcej metódy RSA sa tá istá „tajná informácia“ nachádza na oboch stranách – na strane klienta (na generovanie OTP) a na strane EB (na jeho overenie). (Viac informácií možno nájsť v časti zaoberajúcej sa elektronickým podpisom.)

• SH – statické prístupové heslo

Historicky najstaršia, ale najmenej bezpečná metóda. V tomto prípade autentifikačný údaj predstavuje statické prístupové heslo. V niektorých systémoch si klient môže toto heslo meniť, resp. použiť súbor statických hesiel z tzv. grid karty (GC) podľa výzvy systému EB. U klienta s minimálnou frekvenciou transakcií môže súbor hesiel predstavovať o niečo vyššiu bezpečnosť voči tretej strane než jedno heslo. Niekedy (napr. pri komunikácii s operátorom Call Centra) sa táto autentifikácia doplní o tzv. kontrolné (záložné) otázky.

ŠIFROVANIE. Šifrovanie údajov zabezpečuje ich dôveryhodnosť a ochranu voči tretej strane. Na tento účel sa môžu využiť štandardné protokoly, napr. SSL pri Internet bankingu, WTLS pri WAP bankingu, šifrovanie prenosu medzi SMS centrom a mobilným telefónom v rámci štandardu siete GSM pri SMS bankingu. Niektoré riešenia EB v určitých distribučných kanáloch (napr. Home banking, Mobil banking, Internet banking, SMS banking) majú implementované vlastné šifrovanie na báze niektorej symetrickej kryptovacej metódy (DES, TripleDES, Blowfish, IDEA, Safer atď.) s dĺžkou kľúča 56 až 128 bitov. Kryptovací kľúč pri pokročilejších systémoch je pre každé spojenie iný. V prípade pasívneho E-mail bankingu sa často využíva šifrovanie pomocou produktu PGP alebo komprimácia s heslom (ZIP, ARJ a pod.).

Niektoré distribučné kanály (napr. Telefón a Fax banking) v snahe o technickú

	Autentifikácia		Bezpečnosť prístupu do systému EB	
	Tajná informácia na vytvorenie autentifikačného údaj		Ochrana voči	
	Je výlučným tajomstvom podpisovateľa	Pri komunikácii s EB sa prenáša	3. strane Útočník zvonku	2. strane Útočník z banky
RSA	Áno	Nie	Vysoká	Vysoká
OTP	Nie	Nie	Dostatočná	Záleží na implementácii
SH	Nie	Áno	Nedostatočná	Nedostatočná

PRVKY BEZPEČNOSTI. Jednotlivé bezpečnostné požiadavky, kladené na systém EB, riešia nasledujúce bezpečnostné prvky:

- autentifikačný údaj
- šifrovanie
- elektronický podpis
- archív

Bezpečnosť EB ako celku bude závisieť od bezpečnosti jednotlivých jeho bezpečnostných prvkov:

AUTENTIFIKAČNÝ ÚDAJ. Kontrolovaný prístup do systému EB pozostáva z identifikácie („predstavenie sa“), autentifikácie (overenie totožnosti) a autorizácie (pridelenie práv v systéme EB). Na overenie totožnosti sa v EB využívajú tri druhy autentifikačných údajov, lišiace sa hlavne bezpečnostnou úrovňou a spôsobom ich vytvárania:

• RSA – metóda súkromného a verejného kľúča

V tomto prípade je autentifikačný údaj pri každom prístupe do systému EB iný. Je ním elektronický podpis, vytvorený k náhodnej informácii, ktorú banka poslala klientovi pri prihlasovaní sa do systému EB. Po kontrole správnosti elektronického podpisu má klient umožnenú prácu so systémom EB. (Viac informácií k tejto metóde možno nájsť v časti zaoberajúcej sa elektronickým podpisom.)

• OTP – jednorazové (dynamické) heslo

Aj v tomto prípade je autentifikačný údaj pri každom prístupe do systému EB iný a predstavuje ho jednorazové prístupové heslo OTP (z angl. One-Time Password), ktoré sa generuje na základe tajnej informácie, poradia OTP a často aj na základe časového údaj. Na rozdiel od predchádzajúcej metódy RSA sa tá istá „tajná informácia“ nachádza na oboch stranách – na strane klienta (na generovanie OTP) a na strane EB (na jeho overenie). (Viac informácií možno nájsť v časti zaoberajúcej sa elektronickým podpisom.)

nenáročno šifrovanie vôbec nepoužívajú. V takom prípade je potrebné kľásť zvláštny dôraz na vysokú bezpečnostnú úroveň autentifikačného údaj, resp. elektronického podpisu pri aktívnych operáciách.

ELEKTRONICKÝ PODPIS. Pri aktívnych bankových transakciách je dôležité zaručiť integritu a autorstvo platobného príkazu, prípadne podobnej informácie. Tieto požiadavky by mal garantovať elektronický podpis. V nasledujúcej časti sa pozrieme, ako sú tieto požiadavky splnené pri štyroch druhoch „elektronického podpisu“, najčastejšie používaných v EB:

• RSA – metóda súkromného a verejného kľúča

Podpisovanie informácie (platobný príkaz, prípadne podobná informácia) na strane klienta jeho súkromným kľúčom a overovanie elektronického podpisu jeho verej-

ným kľúčom na strane banky je v súlade s pripravovaným zákonom.

Aby nemohlo dôjsť k „zámene“ verejného kľúča klienta na strane banky, v niektorých bankách sa robí **certifikácia** verejného kľúča klienta – podpísanie tohto kľúča súkromným kľúčom banky a vystavenie papierového protokolu o odovzdaní verejného kľúča. Protokol obsahuje základné údaje o klientovi a opis jeho verejného kľúča. Podpisu a uchovávajú si ho obe strany – klient i banka. V dobe, keď ešte neexistuje nezávislá registračná a certifikačná autorita, takýto protokol chráni jednu stranu pred druhou.

Je dobré si uvedomiť, že vysoká bezpečnosť tejto metódy platí iba za predpokladu, že si klient dokáže ochrániť svoj súkromný kľúč a ostane splnený predpoklad, že táto informácia (súkromný kľúč klienta) je výlučným tajomstvom jeho majiteľa. Preto by napríklad dvojica kľúčov klienta mala byť **generovaná** na počítači klienta, a nie na počítači banky.

Ak na **uchovávanie** súkromného kľúča klient používa disketu, mal by si ju dôkladne chrániť pred zneužitím a pri vkladani diskety do počítača by mal mať istotu, že na tomto počítači nebol spustený rezidentný program, ktorý dokáže odchytiť samotný súkromný kľúč, prípadne heslo, ktorým býva tento kľúč na diskete chránený. Vysokú bezpečnosť pri uchovávaní i používaní súkromného kľúča poskytuje **čipová karta RSA** v kombinácii s **čítačkou čipových kariet s vlastnou klávesnicou** na zadávanie PIN kódu. PIN chráni kartu pred zneužitím – po troch nesprávnych PIN-och sa karta zablokuje. Súkromný kľúč na čipovej karte nie je možné skopírovať, ako je to v prípade kľúča na diskete. Súkromný kľúč totiž kartu neopúšťa ani pri generovaní elektronického podpisu – podpis sa generuje priamo v tejto procesorovej karte.

Pravidelná výmena kľúčov po vypršaní **platnosti certifikátu** tiež pomáha pri dosahovaní vysokej bezpečnosti elektronického podpisu na báze súkromného a verejného kľúča.

	Integrita informácie		Autorstvo informácie		Bezpečnosť informácie & autorstva	
	Elektronický podpis je funkciou		Tajná informácia na vytvorenie el. podpisu		Ochrana voči	
	Časti informácie	Celej informácie	Je výlučným tajomstvom podpisovateľa	Pri komunikácii s EB sa prenáša	3. strane Útočník zvonku	2. strane Útočník z banky
RSA	Nie	Áno	Áno	Nie	Vysoká	Vysoká
MIC	Áno	Nie	Nie	Nie	Dostatočná	Záleží na implementácii
OTP	Nie	Nie	Nie	Nie	Nedostatočná	Nedostatočná
SH	Nie	Nie	Nie	Áno	Nedostatočná	Nedostatočná

Dĺžka elektronického podpisu na báze RSA, ktorá sa dnes v praxi používa, je maximálne 2048 bitov, t. j. 256 znakov. Na jeho výpočet je potrebný určitý výkon. Podpis sa generuje napr. prostredníctvom aplikácie Home banking, prípadne internetového komponentu (Java applet, ActiveX) v osobnom počítači, resp. v osobnom organizátore (PDA). Takisto sa generuje v čipovej karte RSA, prípadne telefóne GSM so špeciálnou SIM kartou. Je zrejme, že ručné zadávanie takého dlhého elektronického podpisu na klasickom telefóne by v prípade Telefón bankingu bolo komplikované. Jednoduchšie je v tomto prípade využiť autonómne zariadenie spolupracujúce s čipovou kartou RSA a cez reproduktor zariadenia „vypípať“ podpis spolu s celým platobným príkazom do mikrofónu telefónneho prístroja. Pri SMS bankingu, kde dĺžka elektronického podpisu niekoľkonásobne prevyšuje dĺžku samotnej SMS správy, by bolo treba podpis rozdeliť do niekoľkých SMS správ.

• **MIC – jednorázový (dynamický) transakčný kód (Message Integrity Code)** Pri využívaní určitých distribučných kanálov EB (WB, TB, SMS...) sa dnes hlavne z praktického hľadiska dáva prednosť jednoduchšej symetrickej metóde generovania dynamického transakčného kódu MIC (Message Integrity Code). MIC sa podobne ako OTP generuje na základe tajnej informácie, poradia MIC, časového údaj a (navyše oproti OTP) aj na základe časti platobného príkazu (najčastejšie sa do výpočtu MIC berie cieľový účet, suma a podobne).

Aj v prípade MIC sa **tá istá „tajná informácia“** nachádza na oboch stranách a nie je splnený predpoklad o „výlučnom tajomstve

podpisovateľa“. V niektorých implementáciách (skôr softvérového charakteru) môže byť táto tajná informácia v inom tvare na strane banky a v inom na strane klienta. V takomto prípade banka nedokáže vygenerovať MIC, resp. OTP, dokáže ho iba overiť. Ďalší okruh otázok, ktoré súvisia s výlučným tajomstvom (tajnej informácie) podpisovateľa sa týka inicializácie zariadení na generovanie MIC, resp. OTP v banke. Aj v prípade MIC, resp. OTP je na mieste protokolárne odovzdanie určitých údajov medzi klientom a bankou, ako je to pri metóde RSA.

Na výpočet MIC, resp. OTP sa používajú jednorázové PIN kalkulátory (ActivCard, Vasco atď.), resp. softvérová aplikácia pre PC/PDA/mobilný telefón/Java applet. PIN kalkulátor rovnako ako softvérová aplikácia sú proti zneužitiu chránené statickým heslom. V niektorých bankách klient dostane iba zoznam OTP.

Dĺžka MIC, resp. OTP je v praxi maximálne 14 znakov. MIC nie je funkciou celého platobného príkazu a nedá sa použiť na „podpísanie“ akejkolvek informácie.

Poznámka: MIC sa niekedy označuje aj ako MAC alebo CK (certifikačný kód).

• **SH – statické transakčné heslo** V niektorých systémoch EB sa ako elektronický podpis k platobnému príkazu používa statické transakčné heslo, v lepšom prípade jedno zo súboru hesiel grid karty (GC). V niektorých systémoch sa takýmto heslom klientovi sprístupní možnosť zadávať platobné príkazy a jednotlivé platobné príkazy sú už bez podpisu. Transakčné heslo neumožňuje kontrolovať integritu platobného príkazu. Po jeho odchytení hrozí zneužitie tohto hesla.

ARCHÍV. Archív sa nachádza na oboch stranách – v banke i u klienta – a slúži na riešenie sporných situácií a prípadný auditing systému EB. Nachádzajú sa v ňom dôležité vymieňané informácie (platobné príkazy a pod.), elektronické podpisy, resp. elektronické potvrdenky k týmto príkazom a informácie o aktivitách systému v danom čase. O váhe týchto podkladov rozhoduje váha používaných bezpečnostných prvkov – kľúčový je v tomto smere druh elektronického podpisu.

• **Elektronická potvrdenka** Elektronická potvrdenka predstavuje krátku správu banky s časovým údajom o prijatí informácie od klienta. Takáto informatívna potvrdenka (IP) má iba informatívnu hodnotu. Dôkaznú hodnotu má až elektronická potvrdenka, ktorá je doplnená o elektronický podpis banky, vytvorený z pôvodnej informácie klienta a krátkej správy banky s časovým údajom (PP). V distribučných kanáloch, ktoré nemajú možnosť doručiť klientovi takúto elektronickú potvrdenku (napr. TB, WB, SMS), je možné využiť presmerova-

nie zaslania potvrdeniek na iný distribučný kanál, napr. e-mail, resp. fax.

BEZPEČNOSŤ ELEKTRONICKÉHO BANKOVNÍCTVA NA SLOVENSKU. Na lepšie poznanie bezpečnosti elektronického bankovníctva na Slovensku sme si otvorili účet v 10 bankách (Všeobecná úverová banka, Slovenská sporiteľňa, Poštová banka, Tatra banka, Prvá komunálna banka, Istrobanka, Poľnobanka, Devín banka, Komerčná banka, ČSOB) a požiadali sme o poskytnutie všetkých dostupných foriem elektronického bankovníctva. Zaujímali sme sa o použité bezpečnostné prvky z hľadiska možnosti ich prípadného zneužitia z druhej strany (zo strany záškodníka z banky), ako i tretej strany (zo strany záškodníka mimo banky).

Pre názornosť sú uvádzané údaje odlišné farebným pozadím, pričom červená farba predstavuje nedostatočný bezpečnostný prvok (umožňuje zneužitie z druhej a tretej strany), žltá farba predstavuje dostatočne bezpečný prvok (umožňuje zneužitie len z druhej strany) a zelená farba predstavuje bezpečný prvok, ktorý pri dodržaní všetkých bezpečnostných zásad neumožňuje jeho zneužitie z druhej ani tretej strany. Konkrétna situácia v jednotlivých bankách je uvedená v prehľadnej tabuľke.

Z tabuľky je zrejme, že relatívne najbezpečnejším distribučným kanálom sa zdá Home banking, kde väčšina bánk používa na prístup do systému, ako i na podpisovanie aktívnych bankových transakcií elektronický podpis na báze asymetrickej metódy súkromného a verejného kľúča (RSA). Pri Internet bankingu túto metódu podpisovania platobných príkazov používa zatiaľ iba jedna banka, aj keď v tomto konkrétnom prípade by bolo možné namietaf voči nedostatočne prehľadnému spôsobu generovania kľúčov cez internet. Počítač, na ktorom sa generujú kľúče klienta, a proces certifikácie verejného kľúča, ako bolo uvedené, úzko súvisia s výlučným tajomstvom podpisovateľa.

Najmenej intímny distribučný kanálom sa zdá telefón banking. Jednak preto, že z hľadiska zachovania minimálneho technického vybavenia klienta komunikácia klienta s bankou nie je šifrovaná. Ak sa na prístup do systému, prípadne na podpisovanie aktívnej bankovej transakcie používa statické heslo, zdá sa tento distribučný kanál nebezpečný a nedostatočne intímny. Na odpočúvanie telefónnej linky a analýzu tónovej voľby totiž nie sú potrebné špeciálne znalosti ani zariadenia. Väčšina bánk túto nízku bezpečnostnú úroveň posilňuje denným limitom na aktívne operácie.

Ako ďalej vyplýva z tabuľky, relatívne často sa v bankách na Slovensku využívajú symetrické metódy tak na prístup do systé-

Právne otázky

Aj keď slovenská legislatíva v súčasnosti zaostáva v prijatí zákona o elektronickom podpise za ostatnými európskymi štátmi (v ČR bol zákon č. 227/2000 Sb. o elektronickom podpise prijatý 29. júna 2000 a platí od 1. októbra 2000; http://www.mvcr.cz/sbirka/2000/zakony3q.html#castka_68), je zrejme, že aj slovenský zákon sa vo svojej podstate nebude odchyľovať od smernice 1999/93/EC Európskeho parlamentu a rady z 13. 12. 1999 pre elektronické podpisy (http://europa.eu.int/eur-lex/en/lif/dat/1999/en_399L0093.html). V podstate ide o tri základné zásady:

1. Zrovnoprávnenie elektronického a klasického podpisu

2. Elektronický podpis umožňuje identifikovať podpisovateľa vo vzťahu k podpisanej informácii

■ Existuje dvojica kľúčov – tzv. súkromný kľúč a verejný kľúč

■ **Súkromný kľúč** = prostriedok na podpisovanie = informácia, ktorá je **výlučným tajomstvom podpisovateľa**

■ Verejný kľúč = prostriedok na overovanie elektronického podpisu vo vzťahu k podpisovateľovi a podpisanej informácii

■ Certifikát verejného kľúča – potvrdzuje, že podpisovateľ vlastní súkromný kľúč, ktorý zodpovedá verejnému kľúču, pre ktorý sa certifikát vystavuje

3. Elektronický podpis platí iba k informácii, pre ktorú bol vytvorený

■ Elektronický podpis jednoznačne identifikuje podpisajúcu informáciu vo vzťahu k podpisovateľovi

■ Elektronický podpis umožňuje zistiť každú zmenu podpisanej informácie



mu elektronického bankovníctva (OTP), ako i na podpisovanie platobných príkazov (MIC). Tieto symetrické metódy, kde tajná informácia potrebná na podpisovanie nie je výlučným tajomstvom podpisovateľa, sú vo väčšine bánk viazané na použitie jednorázových PIN kalkulatorov, ktoré klienta stoja od 1000 do 2000 Sk. Ak sa na podpisovanie príkazov na úhradu používa OTP, prípadne na výpočet MIC sa berie iba suma transak-

cie, nie je zaručená kontrola integrity príkazu na úhradu, a preto je možná jeho modifikácia (napríklad modifikácia cieľového účtu) zo strany prípadného útočníka.

S výnimkou dvoch prípadov klient na Slovensku dostáva z banky iba informatívnu potvrdenku o prijatí platobného príkazu, čo znamená, že v prípade sporu s bankou mu chýba bankou podpísaný doklad o prijíme platobného príkazu – obdoba

potvrdennej papierovej kópie platobného príkazu.

Zaujímavé sú aj obchodné podmienky a zmluva s klientom. Pretože ich pripravujú právnici banky, je zrejme, že banka sa nimi snaží chrániť voči stratám v prípade zneužitia systému elektronického bankovníctva. Presúvanie zodpovednosti za škodu v dôsledku nedostatočnej obozretnosti klienta je prirodzené. Ak je však prenášaná zodpovednosť na klienta aj v prípadoch, ktoré nemá možnosť ovplyvniť s ohľadom na nedostatočnú bezpečnosť samotného distribučného kanála, je na zváženie základná povinnosť banky – vykonávať bankové obchody obozretné a tak, aby neboli poškodené záujmy jej vkladateľov. Obchodné podmienky a zmluva s klientom by preto mali byť ďalším kompasom pri správnom rozhodovaní klienta.

Poznámka: Uvedené údaje sú platné k 1. 3. 2001. Všade tam, kde je RSA uvedené tučným písmom, umožňuje daný systém používať aj procesorové čipové karty RSA (RSA smart cards)

Legenda:

autentiz.	autentizácia (autentifikačný údaj, autentifikácia)
RSA	asymetrická metóda využívajúca súkromný (tajný) a verejný kľúč
OTP	metóda jednorazových hesiel – One Time Password
GC	grid card (metóda niekoľkých statických hesiel)
SH	statické heslo
TC	telefónne číslo mobilného telefónu, resp. klasickej linky
–	bezpečnostný prvok nie je implementovaný, pretože nie je nutný (napr. banka neponúka možnosť aktívne sa prihlásiť)
šifrovanie	šifrovanie prenosu informácií medzi klientom a bankou
S	šifrovaný kanál nejakou šifrou
SSL	šifrovanie cez SSL
WTLS	šifrovanie cez WTLS
PGP	šifrované dáta pomocou produktu PGP (založený na asymetrickej kryptografii)
ZIP	heslom chránený (šifrovaný) archív (zip, arj, rar a pod.)
0	bezpečnostný prvok nie je implementovaný
el. podpis	elektronický podpis aktívnych transakcií (napr. platobného príkazu)
RSA	asymetrická metóda využívajúca súkromný (tajný) a verejný kľúč
MIC	symetrická metóda elektronického podpisu – Message Integrity Code (používajú sa aj pojmy MAC, resp. CK – certifikačný kód)
OTP	metóda jednorazových hesiel – One Time Password
GC	grid card (metóda niekoľkých statických hesiel)
SH	statické heslo
0	bezpečnostný prvok nie je implementovaný, pričom by mal byť implementovaný
–	bezpečnostný prvok nie je implementovaný, pretože nie je nutný (napr. banka neponúka taký typ transakcie, ktorý ho vyžaduje)
potvrdenka	elektronická potvrdenka aktívnej transakcie (napr. platobného príkazu)
IP	informatívna potvrdenka z banky
PP	elektronicky podpísaná potvrdenka z banky (RSA)
–	bezpečnostný prvok nie je implementovaný, pretože nie je nutný (napr. banka neponúka taký typ transakcie, ktorý ho vyžaduje)

		HB	MoB	IB	WB	IVR	CC	SMS	E-mail	Fax
banka 1	autentiz.	RSA		SH		SH	SH	TC+SH	–	TC
	šifrovanie	S		SSL		0	0	S	0	0
	el. podpis	RSA		–		0	0	SH	–	–
	potvrdenka	PP		–		IP	IP	IP	–	–
banka 2	autentiz.	RSA		SH/OTP		SH/OTP		TC	–	TC
	šifrovanie	S		SSL		0		S	ZIP/PGP	0
	el. podpis	RSA		GC/MIC		GC/MIC		–	–	–
	potvrdenka	IP		IP		IP		–	–	–
banka 3	autentiz.	RSA		SH	SH	SH	SH	TC+SH	–	TC
	šifrovanie	S		SSL	WTLS	0	0	S	0	0
	el. podpis	RSA		OTP	OTP	–	0/-	MIC	–	–
	potvrdenka	IP		IP	IP	–	IP	IP	–	–
banka 4	autentiz.	OTP		SH/GC/OTP			SH+GC	TC+SH	–	
	šifrovanie	S		SSL			0	S	0/ZIP	
	el. podpis	0		0/GC/OTP			GC	SH	–	
	potvrdenka	IP		IP			IP	IP	–	
banka 5	autentiz.	OTP		SH	SH			TC	–	SH
	šifrovanie	S		SSL	WTLS			S	S	0
	el. podpis	0/MIC		RSA	0			–	–	–
	potvrdenka	IP		IP	IP			–	–	–
banka 6	autentiz.	RSA		SH/OTP		SH/OTP		TC	–	TC
	šifrovanie	S		S ?		0		S	0	0
	el. podpis	RSA		MIC		MIC		MIC	–	–
	potvrdenka	IP		IP		IP		IP	–	–
banka 7	autentiz.	RSA		SH/OTP		SH		TC		
	šifrovanie	S		S ?		0		S		
	el. podpis	RSA		MIC !		–		–		
	potvrdenka	IP		IP		–		–		
banka 8	autentiz.	RSA		SH/OTP		SH		TC	–	
	šifrovanie	S		S ?		0		S	ZIP	
	el. podpis	RSA		MIC		–		SH/MIC	–	
	potvrdenka	IP		IP		–		IP	–	
banka 9	autentiz.	RSA		OTP				TC	–	
	šifrovanie	S		S ?				S	0	
	el. podpis	RSA		MIC				–	–	
	potvrdenka	PP		IP				–	–	
banka 10	autentiz.	RSA					SH	TC+SH		TC
	šifrovanie	S					0	S		0
	el. podpis	RSA					0	–		–
	potvrdenka	IP					IP	–		–
EB UNICOM	autentiz.	RSA	RSA	RSA/OTP	OTP	OTP	OTP	TC + OTP	RSA	TC + OTP
	šifrovanie	S	S	SSL	WTLS	0	0	S	ZIP/S	0
	el. podpis	RSA	RSA	RSA	MIC	MIC	MIC	MIC	RSA	MIC
	potvrdenka	PP	PP	PP	PP	PP	PP	PP	PP	PP

Ing. Radimír Rexa, CSc., Ing. Roman Papšo,
Ing. Radovan Schreiber
UNICOM, s. r. o.