

Vývoj Homebankingu v naší firmě započal již roku 1994. Od začátku se vyznačoval vysokou mírou bezpečnosti a snadnou ovladatelností. Je určený především pro firmy. Předpokládáme, že firmy používají ekonomické programové vybavení - nějaký typ účetnictví. Účetnictví je určeno pro následné zpracování platebního styku. Homebanking by ho měl pouze bezpečně zprostředkovat a přitom "moc nezdržovat".

Programové vybavení tvořící systém Homebankingu je rozdělen do dvou částí - klient a server.

Klient

základní vlastnosti:

- Bezpečnost
- Možnost připojení přes různá přenosová média včetně Internetu
- Potvrzení přijetí plateb
- Snadné napojení na účetní programové vybavení
- Přidělení různých privilegií různým pracovníkům v rámci firmy
- Modulárnost

Možnost připojení přes různá přenosová média včetně Internetu

Pro šifrovaný přenos údajů se používá protokol na aplikační vrstvě TCP/IP. Principiálně lze tedy použít jak přímé spojení na server banky tak i Internet.

Potvrzení přijetí plateb

Platby jsou potvrzovány v rámci jedné relace. Klient je tedy informován o přijetí platby bankou. V rámci implementace je klient upozorněn na formální nedostatky v platebním příkaze (z účetního SW). Toto upozornění se samozřejmě netýká platby, která je formálně správně ale např. číslo účtu příjemce neexistuje (převod do jiné banky přes clearing ČNB).

Snadné napojení na účetní programové vybavení

Vnitřní formát dat je přizpůsobený ABO formátu. ABO formát byl provozován ČSSB a převzaly ho komerční banky, které vznikly po roce 1989. Tento formát obsahuje většina účetních programů.

Přidělení různých privilegií různým pracovníkům v rámci firmy

Systém umožňuje přidělit uživatelům různý stupeň privilegií při práci s homebankingem:

- Přístup do systému
Uživatel může pouze otevřít program. Uvidí pouze historii stavu na účtu
- Komunikace
Uživatel může spustit komunikaci ze serverem banky. Uvidí aktuální stav
- Elektronický podpis
Uživatel může použít mechanismus elektronického podpisu. Může poslat platební příkaz

Modulárnost

Klientský program se skládá z několika programových modulů které lze spouštět samostatně

- Hlavní programový modul Klient (nejnovější verze Klient 3.7)
Programový modul umožňuje zadávání korunových platebních příkazů a sledování pohybu na účtu. Kromě toho spouští další programové moduly
- Modul zahraničních plateb (nejnovější verze Klient 3.6z)
Modul umožňuje vést cizoměnový účet
- Přenosový programový modul (nejnovější verze Přenos 3.0 TCP/IP)
Modul umožňuje přenos zabezpečeným kanálem. Modul lze použít samostatně. Je možné ho zakomponovat do jiné aplikace např. účetnictví.
- Bezpečnostní modul (nejnovější verze Podpis 3.0)
Modul umožňuje provést elektronický podpis. Modul lze použít samostatně. Je možné ho zakomponovat do jiné aplikace např. účetnictví.
- Nastavení parametrů - včetně vytvoření páru VK/TK (nejnovější verze Uživatel 3.0)
Modul umožňuje zadávání identifikace klienta, změnu hesel, nastavení privilegií a práci s VK/TK (veřejný/tajný klíč) klienta a VK serveru banky. Modul lze použít samostatně. Je

možné ho zakomponovat do jiné aplikace např. účetnictví.

Server

programové vybavení určené pro server se skládá z následujících částí:

- Komunikační server
- Autentizační server
- Modul Správce

Komunikační server - spolupracuje s autentizačním serverem

Komunikační server umožňuje navázání spojení na definované TCP/IP adrese a portu zabezpečeným protokolem. Po navázání spojení na úrovni TCP/IP je tedy v první fázi spojení směrováno na autentizační server. Pokud je spojení autorizováno vytváří se podproces, který dále spojení řídí.

Ochrana vlastního počítače - serveru banky proti útokům s Internetu je věcí implementace. Každopádně na portu, který je přiřazen homebankingu nesmí být povolena žádná jiná služba.

Autentizační server

Autentizační server obsahuje především veřejné klíče klientů. V jeho databázi jsou umístěny i přihlašovací jména firem. Jeho hlavní funkcí je samozřejmě autentizace spojení. Kromě toho však provádí kontrolu elektronického podpisu, kontrolu oprávněnosti klienta pro manipulaci s účtem a kontrolu formálních chyb platebního příkazu.

Modul Správce

Spravuje autentizační server. Modul umožňuje generování páru VK/TK banky a registraci VK klientů. O registraci je vytištěn doklad. Doklad by měl podepsat klient podle podpisového vzoru. Platnost elektronického podpisu je časově omezena (záleží na klientovi). Doklad slouží bance k prokázání platnosti veřejného klíče klienta - neodmítnutelnost zodpovědnosti klienta za platební příkaz. V případě nutnosti např. zcizení počítače klienta, je možné přístup ke službě zablokovat.