

Všechny produkty naší firmy se vyznačují nejvyšší možnou mírou bezpečnosti.

Bezpečná autentizace (prokázání totožnosti) uživatele. Systém bezpečně identifikuje a autentizuje uživatele (klienta) pomocí hesla a veřejného klíče klienta. Autentizací je zajištěno to, že transakce může provádět pouze samotný klient, který zná heslo (nebo vlastní soukromý klíč klienta) a nikdo jiný.

Bezpečné utajení (důvěrnosti) přenášených dat. Utajení je dosaženo pomocí šifrování zpráv. Mechanismus utajení zajišťuje, že žádná třetí osoba nemá možnost přístupu k informacím, přenášeným mezi serverem a klientem.

Zajištění integrity (celistvosti) přenášených dat. Mechanismus zajištění integrity zaručuje, že informace, přenášené mezi serverem a klientem nemohou být změněny ani podvrženy případným útočníkem.

Elektronický podpis důležitých dokladů. Elektronický podpis dovoluje, aby klient mohl provádět finanční transakce vzdáleně, pomocí počítače. Tento mechanismus dovoluje odesílateli zprávy (v našem případě klientovi) "podepsat" zprávu elektronickým podpisem tak, že příjemce zprávy (v našem případě server) může jednoznačně prokázat, že zprávu odeslal a podepsal právě tento klient. Ve spojení se smlouvou o vzájemném uznávání elektronických transakcí, kterou předem uzavřela server s klientem, může server jednoznačně prokázat, že klient transakci provedl a klient se nemůže zbavit zodpovědnosti za provedenou transakci. Mechanismus elektronického podpisu také jednoznačně určí, zda zpráva byla odeslána skutečně klientem a nikoli případným útočníkem.

Ochrana úložiště tajného klíče. Tajný klíč je z hlediska bezpečnosti na straně klienta nejdůležitější parametr. Tajný klíč je proto uložen zašifrovaný. V případě použití I-Key je ochrana klíče maximální. K elektronickému podpisu dochází přímo v něm. Případný útočník by tedy musel mít (fyzicky ukrást) I-Key a navíc by musel znát jeho přístupové heslo.

Jednotlivé bezpečnostní parametry jsou implementovány pro naše produkty různými-nejoptimálnějšími technologiemi.

HomeBanking

U této služby se nepředpokládá stálé napojení na Internet. Předpokládá zpracování většího objemu dat, většinou firemních účtů. Umožňuje propojení s účetním programem. Stálé napojení na Internet by bylo časově náročné a není tedy žádoucí.

Pro vlastní spojení se používá symetrické šifrování 3DES. Klíč pro tento typ šifrování je generován pro každé spojení znovu - klíč relace. Klíč je přenášen šifrovaný pomocí jednoho z klíčů asymetrického šifrování. Asymetrické šifrování je zajištěno systémem na bázi RSA.

Podrobný popis celého systému není tajný. Předmětem utajení je pouze jeden z jeho parametrů - tajný klíč. Podrobnosti o implementaci lze získat na základě e-mailového dotazu.

InternetBanking

Práce s bankovním účtem prostřednictvím InternetBankingu se děje výhradně na Internetu. Jako základní technologie pro spojení byla použito SSL. Pro elektronický podpis a nadřazeného protokolu bylo použito vlastní technologie ComTech (užití principů z Homebankingu)