4 Platební systémy

Platební systémy slouží k převodu peněz z účtu strany A na účet strany B. Nás pochopitelně budou zajímat elektronické systémy, v nichž se zaměříme na systémy využívající kryptografii. V této kapitole se blíže seznámíme s internetovým bankovnictvím, s protokolem 3D Secure, se sítí Bitcoin a nakonec s platebními kartami. Chceme-li uvedené systémy stručně charakterizovat, tak pomocí internetového bankovnictví může majitel účtu (dále klient) spravovat peníze na svém účtu, protokol 3D Secure klientům slouží zejména k platbám nákupů přes internet, síť Bitcoin se používá k platbám pomocí kryptoměny a platební karty se nejčastěji používají k bezhotovostním platbám nákupů v prodejnách.

Platební systém je prakticky specifickým druhem přístupového systému, přičemž aktivy jsou peníze na účtu klientů. Každý klient, z jehož účtu se převod provádí, (tzv. plátce) hraje roli autority, klient na jehož účet převáděné peníze směřují (tzv. příjemce) je fakticky žadatelem a platební systém (obvykle systém bank) hraje roli přístupového systému.

4.1 Internetové bankovnictví

Internetové bankovnictví je elektronický systém, který klientům umožňuje vzdálenou správu peněz na jejich účtu. Prostřednictvím uvedeného systému mohou klienti kontrolovat stav svého účtu a bance zadávat platební příkazy, jimiž se převádějí peníze z jejich účtu na jiný účet.

Internetové bankovnictví je založeno na komunikaci webového prohlížeče klienta s webovým serverem banky. Tato komunikace probíhá pomocí protokolu HTTP, který je kryptograficky zabezpečen nám již dobře známým protokolem TLS. Server banky se autentizuje pomocí svého certifikátu a klient se autentizuje ve vytvořeném TLS spojení obvykle pomocí hesla.

Pokud klient zadá bance příkaz provést převod peněz ze svého účtu na jiný (tzv. transakce), tak je serverem banky vyzván, aby zadanou transakci nějakým způsobem potvrdil. Často server banky zašle pomocí SMS („Short message service“) na telefon klienta potvrzovací číslo („Transaction Authentication Number“ – TAN). Jedná se o náhodné číslo, které pak klient zapíše do příslušné kolonky webového formuláře a toto číslo bance odešle. Ta přijatou hodnotu porovná s hodnotou, která byla uživateli zaslána a v případě shody je transakce provedena. Použitím potvrzovacího čísla se zvyšuje bezpečnost internetového bankovnictví, neboť útočník musí k úspěšnému útoku získat nejen heslo uživatele, ale i telefon uživatele. Z hlediska zabezpečení je v námi popsaném případě uživatel autentizován dvakrát – při přihlášení jde o autentizaci heslem a při potvrzování transakce jde o autentizaci hardwarem. Tato dvojí autentizace se často označuje jako tzv. dvoufaktorová autentizace.

Některé banky používají k potvrzování transakcí namísto telefonu zařízení, které nazveme potvrzovací kalkulátor. Tyto kalkulátory generují potvrzovací číslo buď na základě náhodné výzvy N,

kterou jim banka zašle, nebo na základě aktuálního času t. V ČR banky často používají potvrzovací kalkulátor RSA SecurID (obr. 4.1), v němž se využívá aktuální čas t.

Obrázek 4.1: Potvrzovací kalkulátor RSA SecurID (autor obrázku Mgr. Rudolf Burda)

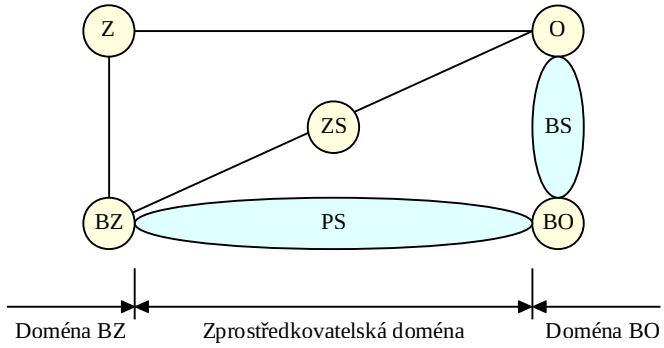
Princip je takový, že klientovi U je při založení účtu vydán potvrzovací kalkulátor s unikátním klíčem K_U. Tento kalkulátor i server banky mají synchronně jdoucí hodiny, takže aktuální čas na serveru je stejný jako na kalkulátoru. Kalkulátor s každou novou minutou vezme aktuální hodnotu času t, vypočítá k ní pečeť $P = \mathrm{PCT}(t, K_U)$ a vypočítanou hodnotu P zobrazí na svém displeji. Klient se v případě potvrzování nějaké transakce podívá na displej svého kalkulátoru a aktuální hodnotu pečeti odešle serveru banky. Server podle identifikátoru přihlášeného klienta zjistí klíč K_U a vypočítá kontrolní hodnotu pečeti $P' = \mathrm{PCT}(t, K_U)$. Pokud platí, že $P = P'$, tak je zaručeno, že protistrana disponuje potvrzovacím kalkulátorem klienta U a jedná se tedy o potvrzení zaslané klientem U.

4.2 Protokol 3D Secure

Protokol 3D Secure umožňuje zákazníkům s platební kartou platit internetové nákupy. Zde je však zapotřebí upozornit, že platební karty se v protokolu fyzicky vůbec nepoužívají a využívají se jen čísla na nich uvedená. Kryptografickým základem protokolu 3D Secure jsou spoje TLS. V současné době existuje protokol 3D Secure ve své druhé verzi [28], kterou si dále popíšeme. V uvedené verzi je definována varianta, kde zákazník platí pomocí vhodné aplikace (běžící například na smartfonu) a varianta, kde zákazník používá webový prohlížeč. My si vysvětlíme druhou z uvedených variant, a to jak pro scénář bez potvrzení zákazníkem, tak i pro scénář s potvrzením zákazníkem.

Základní prvky infrastruktury pro protokol 3D Secure vidíme na obr. 4.2. Tuto infrastrukturu lze rozdělit na tři domény. První doménu spravuje banka zákazníka BZ a kromě ní do této domény náleží uživatelské stanice zákazníků Z („3DS Client“). Druhou doménu má pod svojí správou banka obchodníka BO. Kromě ní je její součástí také internetový obchod obchodníka O („3DS Requestor“), přičemž obchodník komunikuje se svojí bankou prostřednictvím bankovní sítě BS. Do uvedené domény náleží i platební brána („3DS Server“), ale my si zde popis zjednodušíme a budeme popisovat variantu, kdy je platební brána integrována v serveru obchodníka O. Zbývající, třetí doména zprostředkovává interakce mezi prvky předchozích dvou domén. Tato

zprostředkovatelská doména obsahuje zprostředkovatelský server ZS a platební síť PS. Čáry na našem obrázku reprezentují spoje TLS. V TLS spojích směrem k uživatelské stanici Z se autentizují jen protistrany, tj. server BZ a server obchodníka O. K uvedené autentizaci oba servery používají běžné komerční certifikáty. V ostatních TLS spojích se provádí oboustranná autentizace pomocí veřejných klíčů podepsaných certifikační autoritou zprostředkovatelské domény. Předností doménového řešení je, že každá banka potřebuje dodržovat pouze standard 3D Secure. Ostatní bezpečnostní standardy (jako je například metoda autentizace zákazníků) může ve své doméně každá banka realizovat podle vlastní úvahy.



Obrázek 4.2: Infrastruktura pro protokol 3D Secure

Pokud se na architekturu protokolu 3D Secure podíváme z hlediska přístupových systémů, tak zákazník je zde autorita, aktivem jsou peníze na účtu zákazníka, žadatelem je internetový obchod a banka zákazníka hraje roli přístupového systému. Koncept protokolu je takový, že zákazník nejprve obchodníkovi přislíbí platbu. Prakticky se jedná o autorizaci, tj. o udělení práv k penězům zákazníka. Obchodník se s touto autorizací obrátí na banku zákazníka, tj. na přístupový systém. Banka tuto autorizaci buď přijme a vydá povolení k převodu (tzv. rychlá platba), nebo si nejprve vyžádá přímý příkaz od zákazníka a převod povolí teprve poté. V obou případech pak obchodník předá povolení k převodu své bance, která se postará o samotný převod.

Podrobněji si platbu pomocí protokolu 3D Secure vysvětlíme podle obr. 4.3. Kroky vyznačené souvislými šipkami jsou součástí standardu 3D Secure a čárkované šipky vyjadřují kroky, jejichž obsah si mohou zainteresované strany volit podle svého uvážení.

Zákazník Z si u internetového obchodníka O vybere zboží a objednávku potvrdí. Tím dojde k jeho přesměrování na integrovanou platební bránu, která mu zašle formulář, v němž vyplní své platební údaje. Těmito údaji jsou číslo jeho platební karty, platnost karty a ověřovací kód karty. Odesláním formuláře (na obrázku označeno „*Zaplatím!*“) se spustí běh protokolu 3D Secure. Obchodník O nejprve zformátuje zprávu $Z_1 = (DP, KP)$, kde DP jsou data platby a KP je kontext