

Elektronické platební systémy

Doc. Ing. Karel Burda, CSc.



Program

Elektronické platební systémy

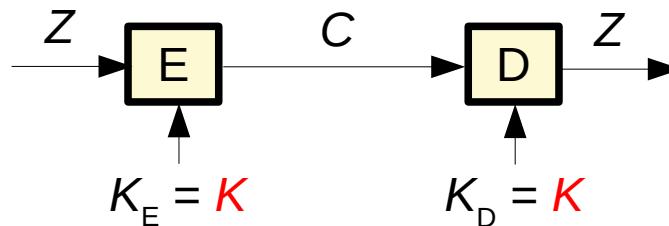
1. Kryptografická primitiva
2. Autentizace v platebních systémech
3. Elektronické platební systémy
4. Obchodní platební systémy
5. Platby kryptoměnou
6. Závěr

1. Kryptografická primitiva

Základní kryptografická primitiva – zajištění důvěrnosti

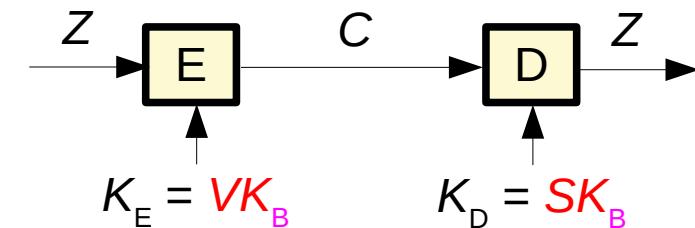
- Důvěrnost zpráv se zajišťuje šifrováním E. Strana A (tzv. odesílatel) zašifrováním zprávy Z vytvoří pseudonáhodnou postupnost $C = E(Z, K_E)$, kde C se nazývá kryptogram a K_E šifrovací klíč. Strana B (opravněný příjemce) invertuje přenesený kryptogram C pomocí dešifrovací funkce D a dešifrovacího klíče K_D do podoby původní zprávy $Z = D(C, K_D)$.
- Osoba bez znalosti klíče K_D nesmí být schopna po stanovenou dobu rezistence T kryptografického systému zjistit, která zpráva Z je v kryptogramu C zašifrována.
- V případě symetrických kryptosystémů platí, že klíč K_D lze z hodnoty K_E za dobu T odvodit, takže se musí utajovat oba klíče. Zpravidla platí, že $K_E = K_D = K$, kde K je tajný klíč, který je sdílen stranami A a B.
- V případě asymetrických kryptosystémů platí, že K_D nelze z hodnoty K_E za dobu T odvodit. Klíč $K_E = VK_B$, resp. $K_D = SK_B$ je tzv. veřejný, resp. soukromý klíč strany B.

Strana A	Kanál	Strana B
----------	-------	----------



Symetrický šifrovací kryptosystém

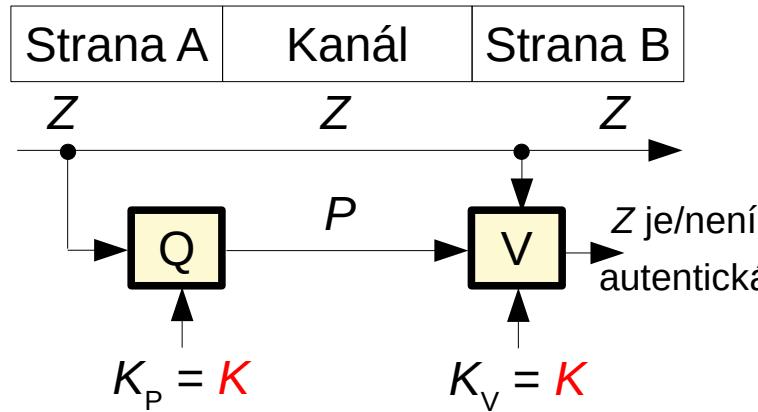
Strana A	Kanál	Strana B
----------	-------	----------



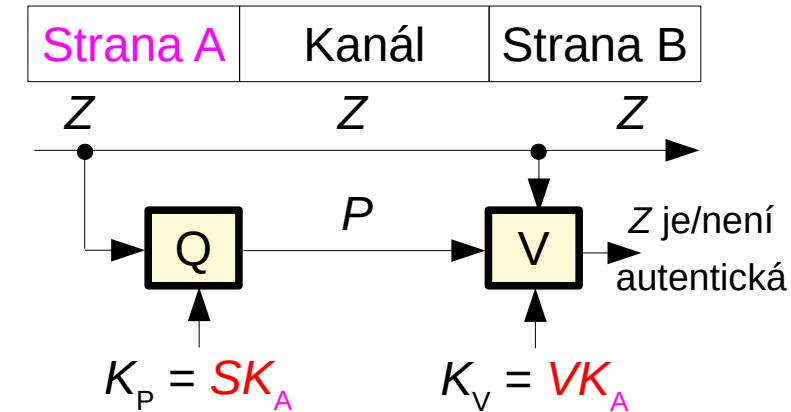
Asymetrický šifrovací kryptosystém

Základní kryptografická primitiva – zajištění autentičnosti

- Autentičnost zpráv se zajišťuje pečetěním Q. Strana A (odesílatel) pečetěním zprávy Z vytvoří krátkou pseudonáhodnou postupnost, tzv. pečet' $P = Q(Z, K_P)$, kde K_P je pečetící klíč. Dvojice (Z, P) je přenesena straně B (příjemci). Ta pomocí ověřovacího klíče K_V a verifikační funkce $V(Z, P, K_V)$ ověří, zda doručená zpráva (Z, P) je autentická, tj. zda ji zaslala strana A.
 - Osoba bez znalosti klíče K_P nesmí být schopna pro libovolnou falešnou zprávu Z' po celou dobu rezistence T systému zjistit její správnou pečet'.
 - V případě symetrických kryptosystémů zpravidla platí, že $K_P = K_V = K$, kde K je tajný klíč sdílený stranou A a B.
 - V případě asymetrických kryptosystémů platí, že $K_P = SK_A$, kde SK_A je soukromý klíč odesílatele A, a že $K_V = VK_A$, kde VK_A je veřejný klíč strany A. Pečet' se zde nazývá podpis.



Symetrický autentizační kryptosystém



Asymetrický autentizační kryptosystém

Symetrické vs. asymetrické kryptosystémy

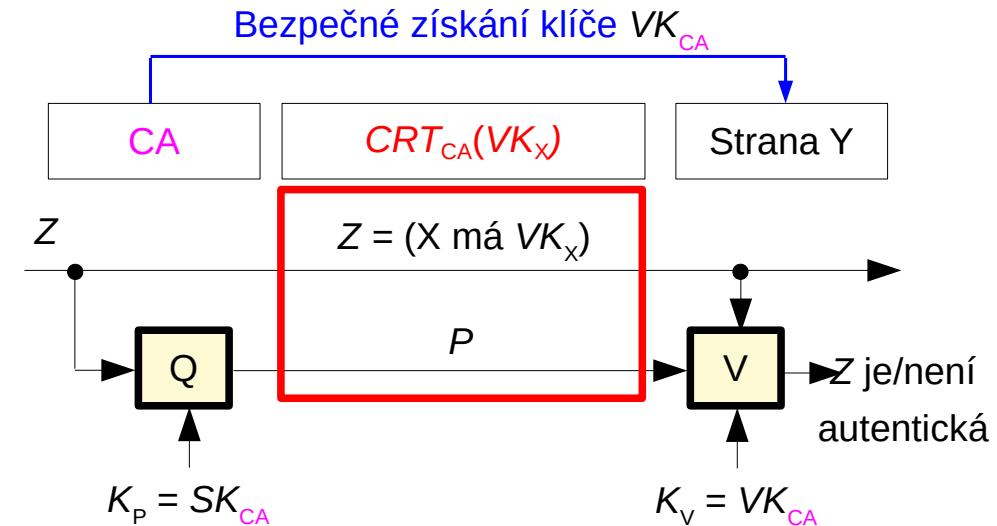
- V případě **symetrických** (jak šifrovacích, tak i autentizačních) kryptosystémů platí, že obě komunikující strany mají **stejný klíč K** . Přesněji řečeno, obecně mohou mít klíče různé, ale jeden klíč lze za dobu rezistence kryptosystému odvodit ze znalosti druhého.
- Výhodou symetrických kryptosystémů je především jejich **rychlost**. Na obou stranách je však klíč tajný a tak problémem u těchto systémů je **bezpečný** přenos klíče protistraně.
- V případě **asymetrických** (jak šifrovacích, tak i autentizačních) kryptosystémů platí, že obě komunikující strany mají **různé klíče**, přičemž platí, že soukromý klíč SK **nelze** ze znalosti veřejného klíče VK odvodit za kratší dobu, než je doba rezistence kryptosystému.
- Nevýhodou asymetrických kryptosystémů je, že oproti symetrickým jsou tisíckrát a více **pomalejší**. Jejich výhodou je **jednodušší** přenos klíče protistraně.
- Jednodušší přenos klíče spočívá v tom, že dejme tomu strana A vygeneruje svoji dvojici SK_A a VK_A a následně veřejný klíč VK_A může v nechráněném kanálu předat protistraně. Při tomto přenosu není zapotřebí zajišťovat **důvěrnost** klíče VK_A (je veřejný), ale jen jeho **autentičnost**. Strana B musí mít záruku, že přijatý klíč VK_A odeslala skutečně strana A.
- V případě **autentizačních asymetrických** kryptosystémů je ještě velkou výhodou tzv. **neodmítnutelnost** podpisu. Strana A, která podepsala nějaký dokument nemůže později tvrdit, že tento podpis není její. Podpis lze totiž vytvořit jen pomocí soukromého klíče SK_A a tím disponuje pouze ona. Pro symetrické autentizační kryptosystémy tato neodmítnutelnost neplatí - správnou pečet' mohou obecně svým klíčem vypočítat obě strany.

Správa klíčů

- Bezpečnost každého kryptografického systému závisí na bezpečnosti jeho klíčů. Tento problém řeší soubor opatření nazývaný **správa klíčů** („Key management“).
- Klíče **symetrického** systému se často distribuují pomocí **kurýrů**. Případně je lze **sjednat** výměnou zpráv po kanálu (Diffie-Hellmanův protokol nebo šifrovaný přenos klíče).
- Bezpečnost **soukromých** klíčů je zajištěna tím, že si je jejich majitel odvodí **sám**.
- Bezpečnou distribuci **veřejných** klíčů zajišťuje **infrastruktura veřejných klíčů** (PKI - „Public Key Infrastructure“). Jejím jádrem je **certifikační autorita CA**, která svým soukromým klíčem SK_{CA} podepisuje zprávy typu „Strana X má veřejný klíč VK_x “. Tato podepsaná zpráva se nazývá certifikát $CRT_{CA}(VK_x)$. Jediným **bezpečně získaným klíčem** VK_{CA} pak uživatelé mohou důvěryhodně získávat veřejné klíče VK_x všech stran, jímž CA vydala certifikát.

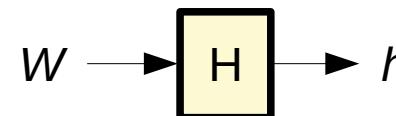
Fungování PKI:

- Strana X si vygeneruje dvojici klíčů SK_X a VK_X . S VK_X jde za CA, které prokáže svoji identitu.
- CA ji vydá $CRT_{CA}(VK_X)$, což je autoritou podepsaná zpráva, že strana X vlastní klíč VK_X .
- Ověřující strana Y si stranou X zasláný $CRT_{CA}(VK_X)$ pomocí bezpečně získaného VK_{CA} ověří a tím důvěryhodně získá VK_X .

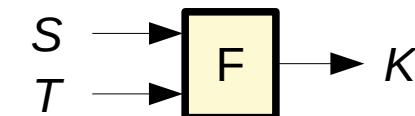


Pomocná kryptografická primitiva

- Kromě již uvedených základních primitiv existují i pomocná primitiva. Jejich účelem je urychlit a zjednodušit fungování kryptografických protokolů.
- K nejpoužívanějším pomocným primitivům patří hešovací a odvozovací funkce.
- Hešovací funkce H přiřadí vzoru W o prakticky libovolné délce tzv. heš h o pevně dané délce (typicky stovky bitů). Heš $h = H(W)$ je obvykle mnohonásobně kratší než vzor W a proto jej v kryptografických protokolech často reprezentuje. Od hešovací funkce se požaduje jednosměrnost (ze znalosti výstupu h nelze určit vstupní W) a bezkoliznost (nelze nalézt různé vstupy W_1 a W_2 takové, aby jejich heše byly stejné).
- Odvozovací funkce F („Key Derivation Function“) přiřazuje tajné hodnotě S (tzv. semeno) a veřejné hodnotě T (tzv. kontext) hodnotu tajného klíče K . Strany, které znají tajné semeno, si veřejně sjednají aktuální kontext T_i (typicky náhodné číslo aktuální relace) a pomocí odvozovací funkce si pro zabezpečení dané relace odvodí unikátní klíč $K_i = F(S, T_i)$.



Hešovací funkce



Odvozovací funkce

2. Autentizace v platebních systémech

Elektronické platební systémy

- Elektronické platební systémy jsou systémy, které umožňují provádět platby a jiné bankovní transakce elektronickými prostředky na dálku.
- Na bankovní transakci se podílí majitel účtu (dále tzv. klient) a banka (tzv. server).
- Základem bezpečnosti elektronických plateb je:
 - důvěrnost přenášených dat,
 - autentičnost přenášených dat,
 - autentičnost komunikujících stran.
- K dosažení těchto požadavků se používají kryptografické techniky a autentizační techniky.
- Kryptografickými technikami se vytvoří bezpečný přenosový kanál, ve kterém se obecně musí komunikující strany navzájem autentizovat.
- Nyní si probereme autentizační techniky v platebních systémech. Některé jsou podobné technikám, které známe z přednášky o systémech EKV, jiné techniky jsou specifické.

Typy autentizace

- U platebních systémů je velkým problémem **autentizace** obou stran.
- **Server** se obvykle autentizuje **v rámci budování kryptografického kanálu** (zpravidla pomocí svého **certifikátu CRT**).
- **Klient** se autentizuje **ve vybudovaném kryptografickém kanálu**. Z přednášky o systémech EKV víme, že v elektronických systémech se používají následující třídy autentizací:
 - a) autentizace **heslem**: klient svoji identitu dokazuje znalostí tajného hesla,
 - b) autentizace **biometrikou**: klient svoji identitu dokazuje svými biometrickými charakteristikami (např. otiskem prstu, hlasem apod.),
 - c) autentizace **hardwarem**: klient svoji identitu dokazuje hardwarem (např. platební kartou, smartfonem apod.).
- V platebních systémech se potkáváme zejména s autentizací pomocí **hesla** a pomocí **hardware**.
- K hardwarovým autentizacím se používají specifická zařízení, která nazveme **autentizační kalkulátory**. Obvykle využívají **symetrickou** kryptografií, kdy v kalkulátoru klienta i v serveru je uložen klientův unikátní **klíč K**. Server v rámci autentizace odešle klientovi unikátní **výzvu V**, z hodnoty výzvy **V** se v kalkulátoru obvykle pomocí vhodné pečetící funkce **Q** odvodí tzv. **odpověď O = Q(V, K)** a ta je předána serveru. Server následně vypočítá kontrolní hodnotu **O' = Q(V, K)**. Pokud **O = O'**, tak je autentizace úspěšná.

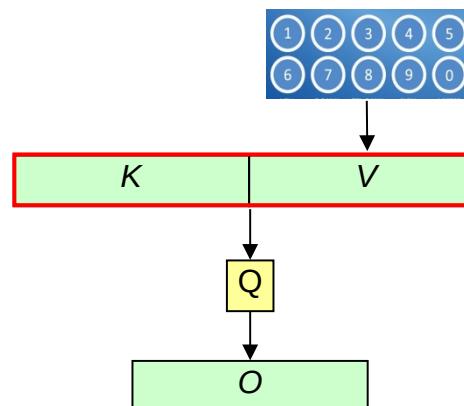
Autentizační kalkulátor bez explicitní výzvy

- Autentizační kalkulátor bez explicitní výzvy zjednodušuje autentizační protokol tím, že výzva **V** není explicitně přenášena.
- Výzva je v tomto případě implicitní a jedná se o **časový údaj t** . Hodiny serveru i klienta jsou synchronní, takže obě strany mají v okamžiku autentizace stejnou hodnotu t .
- Obvykle používanou pečetící funkcí **Q** je **hešovací funkce H**, takže $O = O' = H(K \parallel t)$, kde symbol **||** reprezentuje operaci zřetězení.
- Na obrázku vpravo je autentizační kalkulátor **SecurID**. Často jej používají banky v ČR.



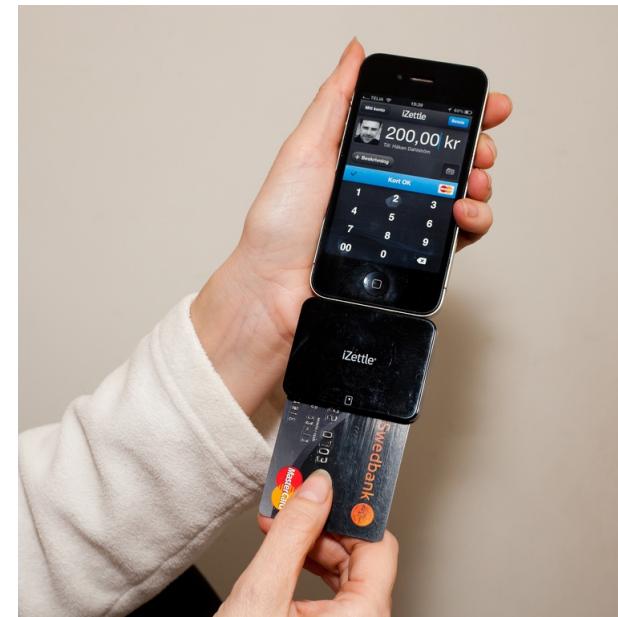
Autentizační kalkulátor s manuálním zadáním výzvy

- Dalším typem autentizačního kalkulátoru je kalkulátor s **explicitní** výzvou, kterou je nutné do kalkulátoru zadat **manuálně**.
- Kalkulátor (viz obrázek vpravo) je vybaven vestavěnou **klávesnicí** a **displejem**. Jako pečetící funkce **Q** se používá symetrická šifra nebo hešovací funkce.
- Uživateli se při přihlášení k serveru zobrazí na obrazovce počítače **výzva V**. Uživatel ji pomocí vestavěné klávesnice přepíše do svého autentizačního kalkulátoru, který následně vygeneruje odpověď **O = Q(V, K)**. Odpověď se zobrazí na vestavěném displeji.
- Žadatel odpověď **O** přepíše do počítače a odešle serveru. Ten klíč kalkulátoru **K** i výzvu **V** zná, takže si přijatou odpověď může **ověřit vlastním výpočtem**.



Autentizační kalkulátor pro platební kartu

- V bankovnictví se často používají autentizační kalkulátory, do kterých se vkládá platební karta (obvykle jsou označovány zkratkou **CAP** - „Chip Authentication Program“).
- Autentizační kalkulátor generuje autentizační odpověď **O** na základě platební **karty** klienta s klíčem **K**, **pinu** platební karty (prakticky se tedy jedná o dvoufaktorovou autentizaci) a popřípadě i nějaké **výzvy** od banky.
- Buď se jedná o samostatné zařízení (obr. vlevo), či periférii smartfonu (obr. vpravo).
- Autentizační kalkulátor typu CAP může pracovat v režimu **bez výzvy** a **s výzvou**.



3. Elektronické platební systémy

Typy platebních systémů

- Elektronické platební systémy lze klasifikovat podle různých kritérií (účel, subjekty apod.)
- Podle typu platebního terminálu lze platební systémy klasifikovat:
 - telefonní: terminálem klienta je telefon,
 - počítačové: terminálem klienta je počítač,
 - bankomatové: terminálem klienta je bankomat,
 - obchodní: terminálem klienta je platební terminál.

Telefoniční platební systémy (1/3)

- U telefonních platebních systémů jsou terminálem **telefony** jak pro pevnou linku, tak i mobilní.
- Nejvíce se tyto systémy používají v **bankovnictví**.
- Autentizace se provádí podle **telefonního čísla** volajícího a je případně doplněna některou z technik autentizačního kódu (např. heslo). Přenášená data zpravidla **nejsou** šifrována.
- V praxi se používají telefonní systémy:
 - a) **hlasové**: Klient zavolá na speciální číslo banky a podle hlasového menu si stiskem kláves volí provádění příslušných operací. Tyto systémy jsou pro svoji pomalost a nepohodlnost postupně rušeny.
 - b) **SMS**: Klient komunikuje s bankou pomocí SMS zpráv přímo (viz dále).
 - c) **datové**: moderní mobilní telefony obsahují i počítač s datovým připojením přes mobilní síť. Ale to se prakticky jedná už o internetové bankovnictví (viz dále).

Telefoniční platební systémy (2/3)

- Kromě bankovních aplikací se v současné době používají mobilní telefony k **přímým platbám** pomocí SMS („Short message service“).
- Obchod nebo firma má uzavřenu **smlouvu** s telefonním operátorem.
- Klient pokud si chce zakoupit nějaké zboží (kávu z automatu, jízdenku na tramvaj apod.), tak zašle svému operátorovi SMS zprávu s **kódem** prodejce, zboží a případně prodejního místa.
- Operátor **převede** odpovídající peněžní částku z účtu svého klienta na účet prodejce a zašle **příkaz k výdeji** daného zboží (např. SMS zprávu pro daný nápojový automat nebo SMS jízdenku na mobilní telefon kupujícího).

Aplikace v telefonu

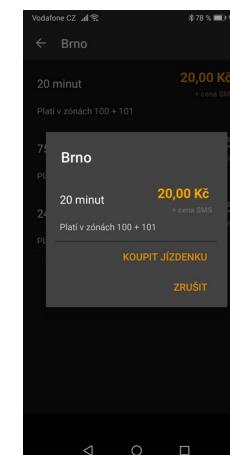


Telefoniční operátor

Nápoj z automatu

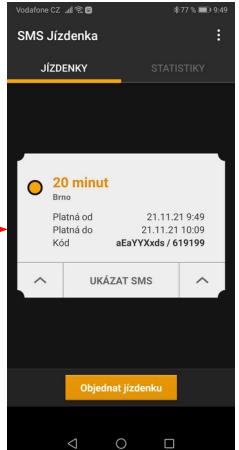


Aplikace v telefonu



Telefoniční operátor

SMS jízdenka



Telefoniční platební systémy (3/3)

- Perspektivním rozšířením telefonních platebních systémů je **integrace** mobilního telefonu a **elektronické platební karty**.
- Elektronická platební karta je prakticky **softwarová aplikace** běžící na procesoru telefonu. Výkonnost tohoto procesoru dovoluje podstatně zvýšit bezpečnost plateb použitím kvalitních **kryptografických** technik.
- Standardní komunikační rozhraní je **GSM**, ale prosazuje se i technologie **NFC** („Near Field Communications“, ISO 18092) což je prakticky mírně modifikovaná komunikační technologie bezdrátových karet (ISO 14443).
- Rozhraní NFC umožňuje velice jednoduše realizovat rutinní platby (např. v obchodě, nebo při vstupu do tramvaje) pouhým **přiložením telefonu ke čtečce**. Čtečka i telefon se navzájem autentizují a poté provedou platbu.



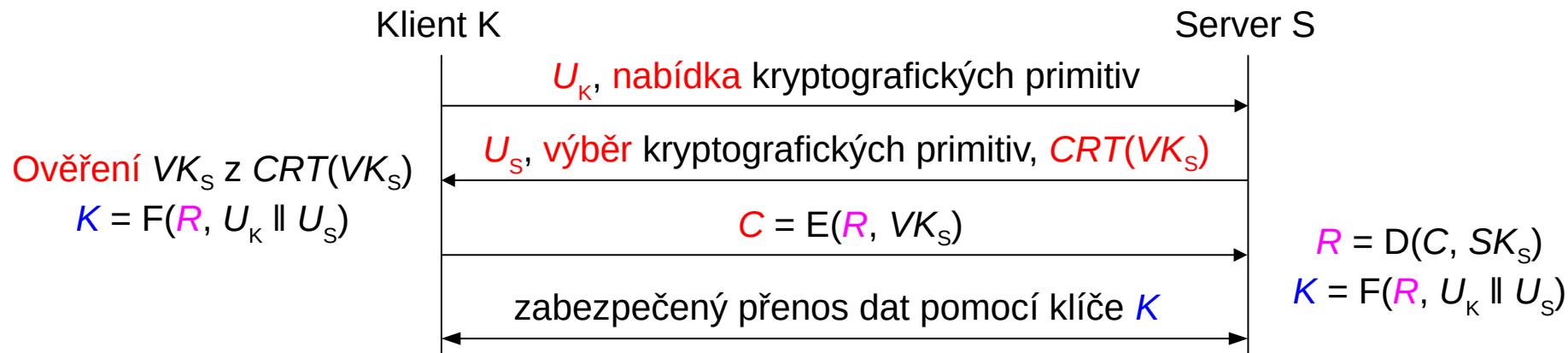
Počítačové platební systémy

- U **počítačových platebních systémů** používají klienti běžný počítač s webovým prohlížečem.
- Tyto platební systémy slouží především k internetovému **bankovnictví** a k internetovému **nakupování**.
- Autentizace klientů se provádí některou z technik autentizačního kódu (zpravidla **heslo**, nebo **certifikát**). Tato autentizace je případně doplněna autentizací zasláním jednorázového kódu platební operace na mobilní telefon („mobile TAN“ - mTAN).
- Důvěrnost i autentičnost dat je zajištěna **kryptografickými protokoly**. K tomu se nejčastěji využívá TLS protokol.



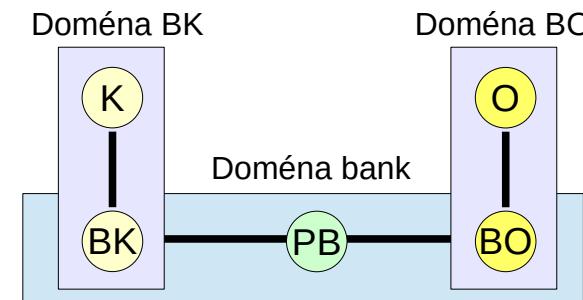
TLS protokol v internetovém bankovnictví

- K zabezpečení webového protokolu **HTTP** se používá kryptografický protokol **TLS** („Transport Layer Security“). Kombinace **HTTP** s **TLS** se označuje **HTTPS**.
- Vytvoření zabezpečeného TLS kanálu (ve verzi 1.2):
 1. Klient K zašle náhodné číslo (tzv. unikát) U_K a **seznam** kryptografických primitiv, které dokáže provádět.
 2. Server banky zašle svůj unikát U_S , kryptografická **primitiva**, která se v transakci použijí a svůj certifikát $CRT(VK_S)$.
 3. Klient z certifikátu ověří VK_S , zvolí náhodné a tajné semeno R a to zašifrovaně zašle jako kryptogram $C = E(R, VK_S)$.
 4. Server dešifruje C a získá R . Obě strany nyní znají tajné semeno R z něhož a z unikátů pomocí odvozovací funkce získají klíč $K = F(R, U_K \parallel U_S)$ pro autentizaci a šifrování dat.
- Server se autentizoval **certifikátem** a klient se později autentizuje **heslem**, které je spolu s ostatními přenášenými daty zašifrováno klíčem K .



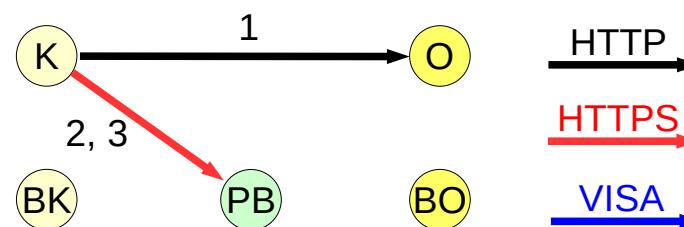
Internetový platební protokol 3D Secure

- Kromě bankovních převodů se k platbě přes internet používá celá řada řešení (např. PayPal). V současné době je velmi rozšířen protokol 3D Secure.
- Protokol **3D Secure** umožňuje platbu klientů obchodníkům přes internet. Základními subjekty protokolu jsou:
 - klient K,
 - obchodník O,
 - banka klienta BK,
 - banka obchodníka BO,
 - platební brána PB:
 - zprostředkovává komunikaci mezi ostatními subjekty,
 - zprostředkovává převod z účtu klienta na účet obchodníka.
- **Banka klienta** se svými klienty tvoří jednu doménu, **banka obchodníka** se svými obchodníky tvoří druhou doménu a **platební brána** se všemi bankami tvoří třetí doménu. Podle těchto **tří domén** nese protokol své jméno (3D = „Three Domain Secure“).
- Komunikace mezi subjekty je protokolem **HTTP**, který je kryptograficky zabezpečen protokolem **TLS**. Tato komunikace se označuje **HTTPS**.
- Výhodou protokolu 3D Secure je, že kryptografické řešení každé domény je sice zcela v kompetenci jejího správce, avšak každá doména přesto může efektivně a bezpečně spolupracovat s ostatními prostřednictvím protokolu **HTTPS**.



Algoritmus protokolu 3D Secure (1/2)

- 1. Klient K si na internetových stránkách obchodníka O vybere a objedná zboží. Tato komunikace je zpravidla nezabezpečeným protokolem **HTTP**. Stisknutím tlačítka „**Platba platební kartou**“ klient spustí protokol 3D Secure. Server obchodníka poté zašle prohlížeči klienta HTTP zprávu s kódem **303, adresou** platební brány a s **daty** pro platbu (zpravidla částka, měna, identifikátor a adresa obchodníka).
- 2. Prohlížeč se na základě kódu 303 a zaslané adresy připojí protokolem **HTTPS** k platební bráně (tzv. přesměrování prohlížeče). Při tomto připojení **předá** i údaje o transakci od obchodníka.
- 3. Klientovi se na monitoru objeví formulář (obr. vpravo), který **doplní** údaje ze své platební karty (číslo karty, platnost karty, bezpečnostní kód karty). Stiskem tlačítka „**Zaplatit**“ zašle tyto údaje platební bráně.

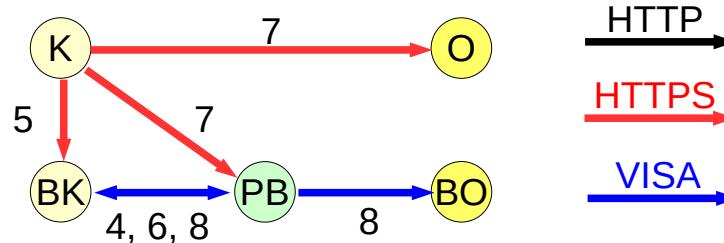


The screenshot shows a secure payment interface:

- Bezpečná platba kartou**: Payment method: VISA.
- Shrnutí vaší objednávky**:
 - Obchodník**: RegioJet / Student Agency, Nam. Svobody 17, 602 00 - Brno (CZ), www.regiojet.cz
 - Číslo objednávky**: 1016630294
 - Celkem**: 420,00 CZK
- Payment Fields**:
 - Umožňuje vaše karta platby na internetu?
 - Číslo vaši karty: [Input field]
 - Platnost karty do: [Input field] / [Input field]
 - Ověřovací kód: [Input field]
- Zaplatit 420,00 czk**: Pay button.
- Logos**: MasterCard, Maestro, VISA, Diners Club International.
- Verifications**: MasterCard SecureCode, Verified by VISA.

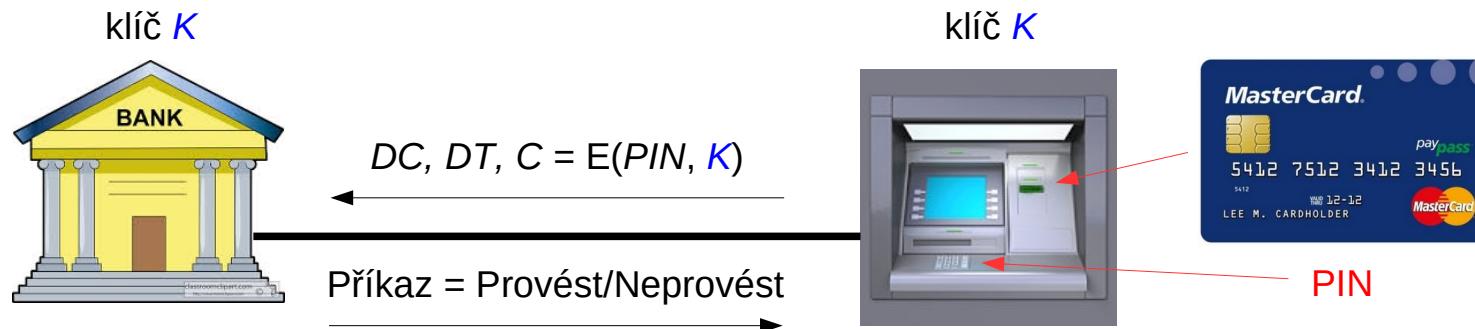
Algoritmus protokolu 3D Secure (2/2)

- 4. Platební brána z čísla karty zjistí banku klienta a zašle ji v chráněné síti bank (na obrázku VISA) potřebné údaje (obvykle částku a identifikátor obchodníka). Následně brána přesměruje prohlížeč na autentizační stránku banky klienta.
- 5. Prohlížeč se protokolem **HTTPS** připojí k serveru banky klienta. Zobrazí se mu **autentizační stránka** (obr. vpravo), kde vidí údaje o transakci a má možnost se své bance autentizovat. Volba techniky autentizace závisí na bance. Často se používá jednorázové heslo zaslané na mobilní telefon klienta (tzv. **mTAN** – varianta na obr. vpravo).
- 6. Po úspěšné autentizaci banka klienta přes chráněnou síť bank informuje platební bránu o **rezervaci částky** pro danou platbu. Prohlížeč klienta je serverem banky **přesměrován** zpět na platební bránu.
- 7. Prohlížeč se protokolem **HTTPS** připojí k platební bráñě, kde se dozví, že platba proběhla úspěšně a je pak přesměrován na obchodníka. Informaci o provedené platbě **předá** platební brána i obchodníkovi. Ten nyní může zboží klientovi zaslat. Tímto protokol končí.
- 8. Ve stanovených intervalech se přes síť VISA provádějí **mezibankovní vyrovnání**, kdy je částka z účtu klienta převedena na účet obchodníka.



Bankomatové platební systémy

- Bankomatové platební systémy slouží klientům k výdeji a ke vkládání hotovosti.
- Jsou tvořeny sítí specializovaných terminálů, tzv. bankomatů, které jsou v neveřejné síti připojeny k bance. Bankomaty sdílejí se svou bankou tajný klíč K .
- K autentizaci klienta se používá kombinace **znalosti** a **vlastnictví** předmětu. Klient vloží do čtečky bankomatu svoji **kartu** a z jejího magnetického proužku se přečtu data o kartě **DC**. Klient pomocí klávesnice bankomatu zadá čtyřmístný číselný **PIN** a následně zadá požadavky na transakci.
- Bankomat zašle bance data o kartě (**DC**), data o transakci (**DT**) a **PIN** zašifrovaný klíčem K do podoby kryptogramu **C**.
- Banka kryptogram **C** dešifruje, ověří správnost pinu, stav účtu a bankomatu zašle příkaz k provedení, resp. neprovedení transakce.



Útoky na bankomaty

- Útočník potřebuje k útoku získat **údaje** na magnetickém proužku karty a **PIN**.
- Údaje z magnetického proužku karty se typicky získávají skrytou čtečkou v podobě nástavce ve štěrbině pro vložení karty (drží jej pravá ruka na obrázku vpravo nahore).
- PIN může získat **falešnou klávesnicí** (v levé ruce) nebo **skrytou kamerou** (obrázky vpravo dole).



Riziková místa bankomatů

Horní nebo boční lišta

Slouží podvodníkům k instalaci kamery pro odpozorování PIN.

Štěrbina pro vložení karty

Zloději na ni, nebo do ní nasazují čtečku magnetického proužku karty, aby ji mohli duplikovat.

Klávesnice

Může být překryta fólií nebo falešnou klávesnicí. Další možnost získání PIN.

Výdej hotovosti

Podvodníci sem nasazují lištu shromažďující bankovky.

Další krok ➔

: Přemysl Souček Grafika: Milan Macháček, Tomáš Průdík



Viz: <http://finweb.ihned.cz/c1-39316960-bankomat-jako-past-na-penize-podivejte-se-na-finty-zlodeju>

Obchodní platební systémy

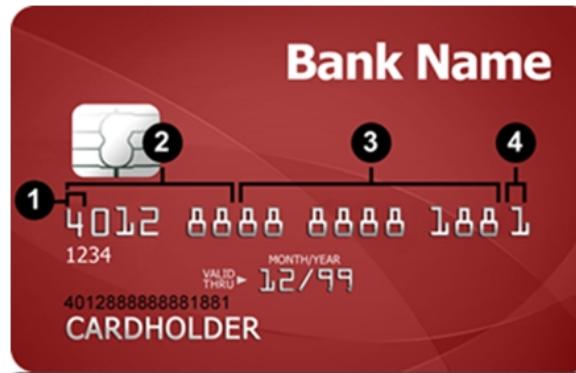
- **Obchodní** platební systémy slouží k elektronické platbě klientů pomocí karty v místech koupě zboží, resp. služby (typicky v obchodech, či prostředcích MHD).
- Terminálem těchto systémů je **čtečka karet** vybavená LCD displejem a případně klávesnicí.
- Při platbě klient bezdrátovou kartu **přiloží** ke čtečce nebo kontaktní kartu **vloží** do čtečky terminálu a případně zadá svůj **PIN**.
- Čip karty **zkontroluje** PIN a buď platbu terminálu **potvrdí** (off-line) nebo přes terminál zašle **dotaz** do banky. Po potvrzení bankou platbu **potvrdí** terminálu (on-line). Podrobnosti jsou na dalších snímcích.
- Obchodník potvrzení karet o platbě **zasílá** bance, která provede převod z účtu zákazníka na účet obchodníka.



4. Obchodní platební systémy

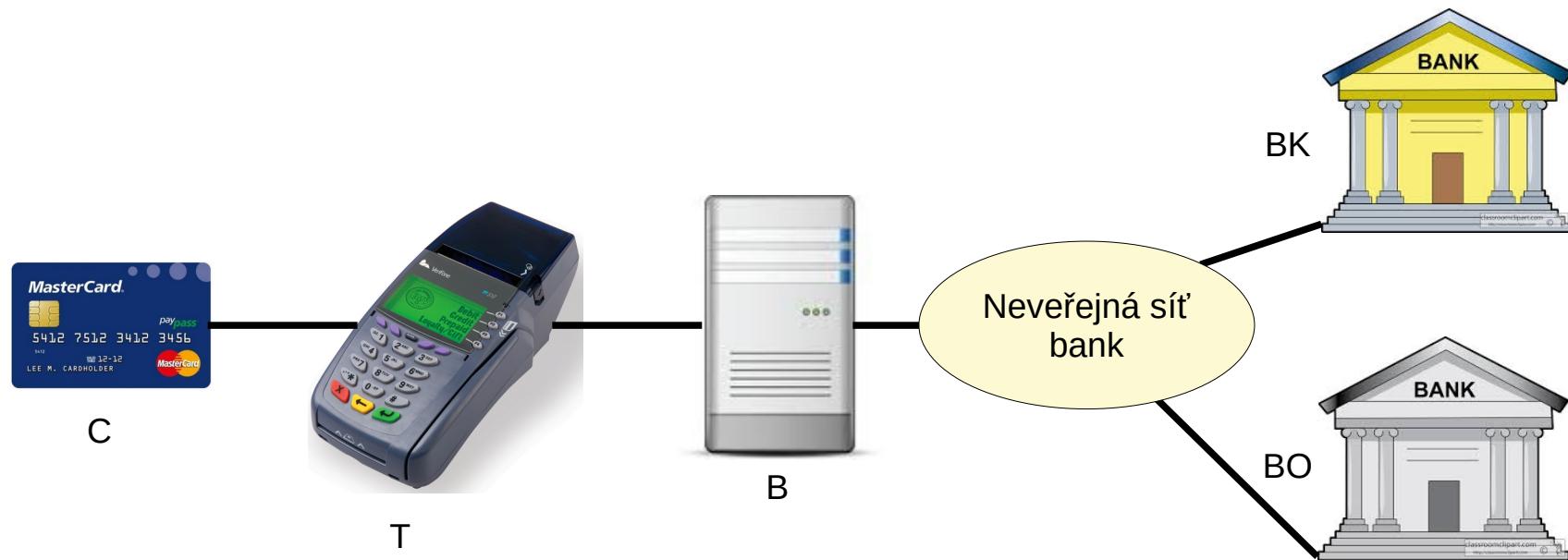
Platební karty

- V současné době se téměř výhradně používají karty s **mikropočítáčem** („Smart Card“). Komunikační rozhraní k čipu je buď **kontaktní**, nebo **bezkontaktní**.
- Z důvodů zpětné kompatibility moderní karty umožňují i starší platební techniky. Jsou proto opatřeny **magnetickým proužkem** a **reliéfními znaky**.
- Platební karta má na líci vyznačen unikátní **číselný identifikátor** (obr. vlevo). V ČR je má tento identifikátor obvykle šestnáct pozic. První číslice (1) identifikuje **obor** použití karty (číslice 4 a 5 jsou pro bankovnictví). Prvních 6 číslic (skupina 2) je identifikátor **banky** („Bank Identification Number“ - **BIN**). Poslední číslice (4) je **kontrolní číslice** celého identifikátoru (počítá se tzv. Luhnovým algoritmem). Zbývající číslice (skupina 3) je číslem **účtu** („Primary Account Number“ - **PAN**).
- Na rubu karty (obr. vpravo) je magnetický **proužek**, **vzor podpisu** držitele karty a **bezpečnostní kód** karty (v červeném kroužku) označovaný CVV2 (u VISA karet) nebo CVC2 (Master Card). Tento kód slouží k platbám přes internet.



Strany kryptografických protokolů platebních karet

- Strany protokolů:
 - **karta C**, kterou vlastní **klient K**,
 - **terminál T**, který vlastní **obchodník O**,
 - **banka klienta BK**,
 - **banka obchodníka BO**,
 - **platební brána B**:
 - zprostředkovává komunikaci mezi terminálem a bankou klienta,
 - zprostředkovává převod z účtu klienta na účet obchodníka.



Kryptografické protokoly platebních karet

- Standardy **EMV** (Europay, MasterCard, Visa) definují kryptografická primitiva a parametry pro platební protokoly karet.



- Banky si ze standardizovaných kryptografických primitiv sestavují **vlastní** protokoly.
- Certifikáty veřejných klíčů bank podepisuje **Certifikační autorita CA** konsorcia EMV svým soukromým podepisovacím klíčem SK_{CA} . V **každém** terminálu je bezpečně uložen VK_{CA} , což je ověřovací klíč CA. Jím terminál může ověřit autentičnost certifikátu libovolné banky.
- Kryptografické klíče:
 - K_C = klíč karty, který zná také banka klienta,
 - VK_C a SK_C = veřejný a soukromý podepisovací klíč karty,
 - VK_{BK} a SK_{BK} = veřejný a soukromý podepisovací klíč banky klienta.
- Data:
 - DC = data karty (identifikátor karty, identifikátor banky, doba platnosti atd.),
 - DP = data platby (částka, měna, identifikátor obchodníka, účet obchodníka atd.).

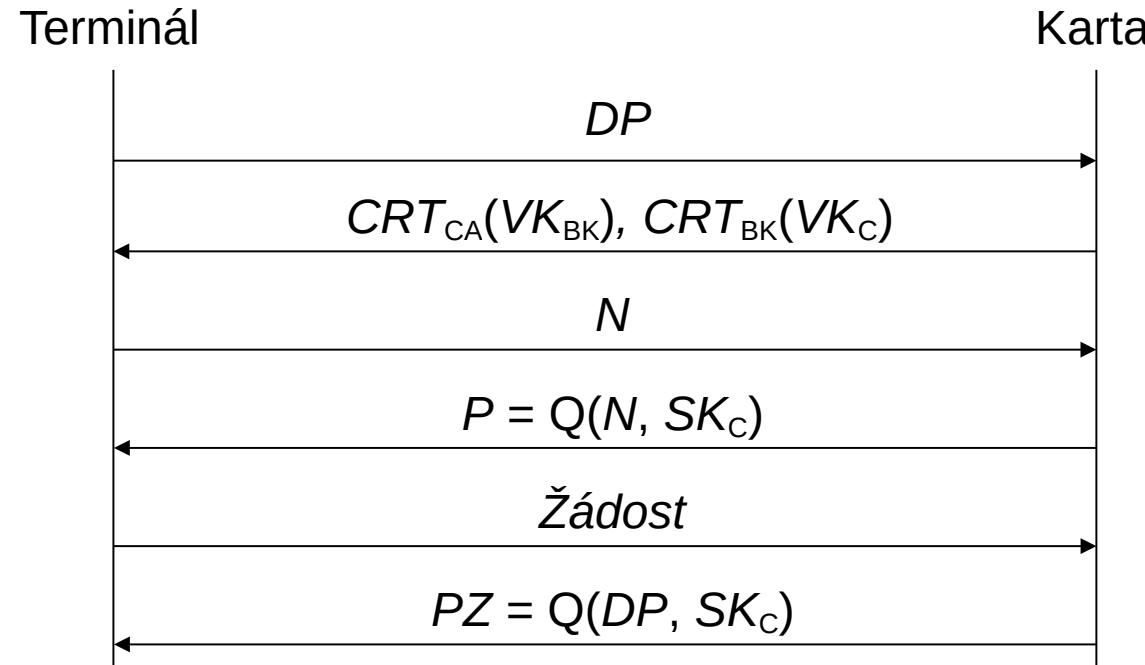
Nespřažený platební protokol (1/3)

- Protokoly obchodních terminálů jsou buď **spřažené** („on-line“), nebo **nespřažené** („off-line“).
- **Nespřažené** platební protokoly se uskutečňují **bez** účasti banky klienta a jsou tak méně bezpečné. Používají se pro platby **malými** částeckami. Karta je tzv. „nabita“ **omezenou** finanční částeckou (tzv. elektronická peněženka). Čerpání této částky kontroluje čip karty.
- Platba se v tomto případě obvykle provádí **bezdrátovou** kartou a **nevkládá** se ani PIN – transakce je tak rychlejší.
- Při autentizaci se používá:
 - $CRT_{CA}(VK_{BK})$: certifikát VK_{BK} podepsaný soukromým klíčem certifikační autority CA,
 - $CRT_{BK}(VK_C)$: data karty DC a VK_C podepsané soukromým klíčem banky klienta BK.
- Terminál pomocí VK_{CA} ověří $CRT_{CA}(VK_{BK})$, čímž ověří autentičnost VK_{BK} .
- Pomocí VK_{BK} se ověří certifikát $CRT_{BK}(VK_C)$, čímž obchodník získá záruku, že zákazník platí kartou vydanou bankou BK. Pokud této bance důvěruje, tak výsledky nespřaženého platebního protokolu (viz dále) přijme.



Nespřažený platební protokol (2/3)

- Schéma protokolu (popis na následujícím snímku):



- Platební brána později předá každou trojici (DC , DP , PZ) příslušné bance BK. Ta z DC identifikuje kartu C a pomocí jejího klíče VK_C a ověří správnost podpisu PZ pro data platby DP . V kladném případě se převede příslušná částka z účtu klienta na účet obchodníka.

Nespřažený platební protokol (3/3)

- Průběh protokolu:
 1. Terminál zašle kartě DP , tj. data k platbě (částka, měna a účet obchodníka).
 2. Karta zašle terminálu $CRT_{CA}(VK_{BK})$ a $CRT_{BK}(VK_C)$. Ten si pomocí uloženého VK_{CA} ověří z $CRT_{CA}(VK_{BK})$ veřejný klíč banky VK_{BK} a tímto klíčem ověří i $CRT_{BK}(VK_C)$. Získá tím důvěryhodně veřejný klíč karty VK_C .
 3. Terminál poté zašle kartě náhodné číslo N .
 4. Karta odpoví podpisem $P = Q(N, SK_C)$ přijatého N .
- 5. Terminál pomocí VK_C ověří podpis P . Tím si ověřil pravost karty – karta zná SK_C , který odpovídá VK_C z certifikátu. Následně kartě zašle žádost o platební závazek PZ .
- 6. Pokud je v elektronické peněžence karty dostatek prostředků, tak karta odešle platební závazek $PZ = Q(DP, SK_C)$, což je její podpis dat k platbě DP .
- Obchodník si pak hromadně (např. za celý den) nárokuje u platební brány na základě trojice (DC, DP, PZ) převody z účtu obslužených klientů na účet svůj.
- Platební brána předá každou trojici (DC, DP, PZ) příslušné bance BK. Ta z DC identifikuje kartu C a pomocí jejího klíče VK_C a ověří správnost podpisu PZ pro data platby DP . V kladném případě se převede příslušná částka z účtu klienta na účet obchodníka.

Útok na nespřažený platební protokol

- Útok na nespřažený platební protokol využívá skutečnost, že tento protokol probíhá **bez aktivní účasti** majitele karty. Pokud tedy útočník propojí čtečku karet platebního terminálu s **cizí platební kartou**, tak může dosáhnout zaplacení své útraty na účet někoho jiného.
- **Útočník** se svým **komplicem** si vyhlédnou **oběť** s platební kartou. Komplic nenápadně ke kartě oběti (umístěně např. v zadní kapse kalhot) přiblíží **čtečku**. Ta je bezdrátově propojena s komunikačním **rozhraním**, které je ukryto v jinak nefunkční kartě útočníka.
- Útočník provede **objednávku** a k platebnímu terminálu obchodníka přiloží svoji „**kartu**“. Tím dojde k bezdrátovému propojení platebního terminálu s kartou oběti. Platební protokol proběhne automaticky a oběť tak nevědomky zaplatí útratu útočníka.

Útočník s
komunikačním
rozhraním



Spoj

Komplic se
čtečkou karet



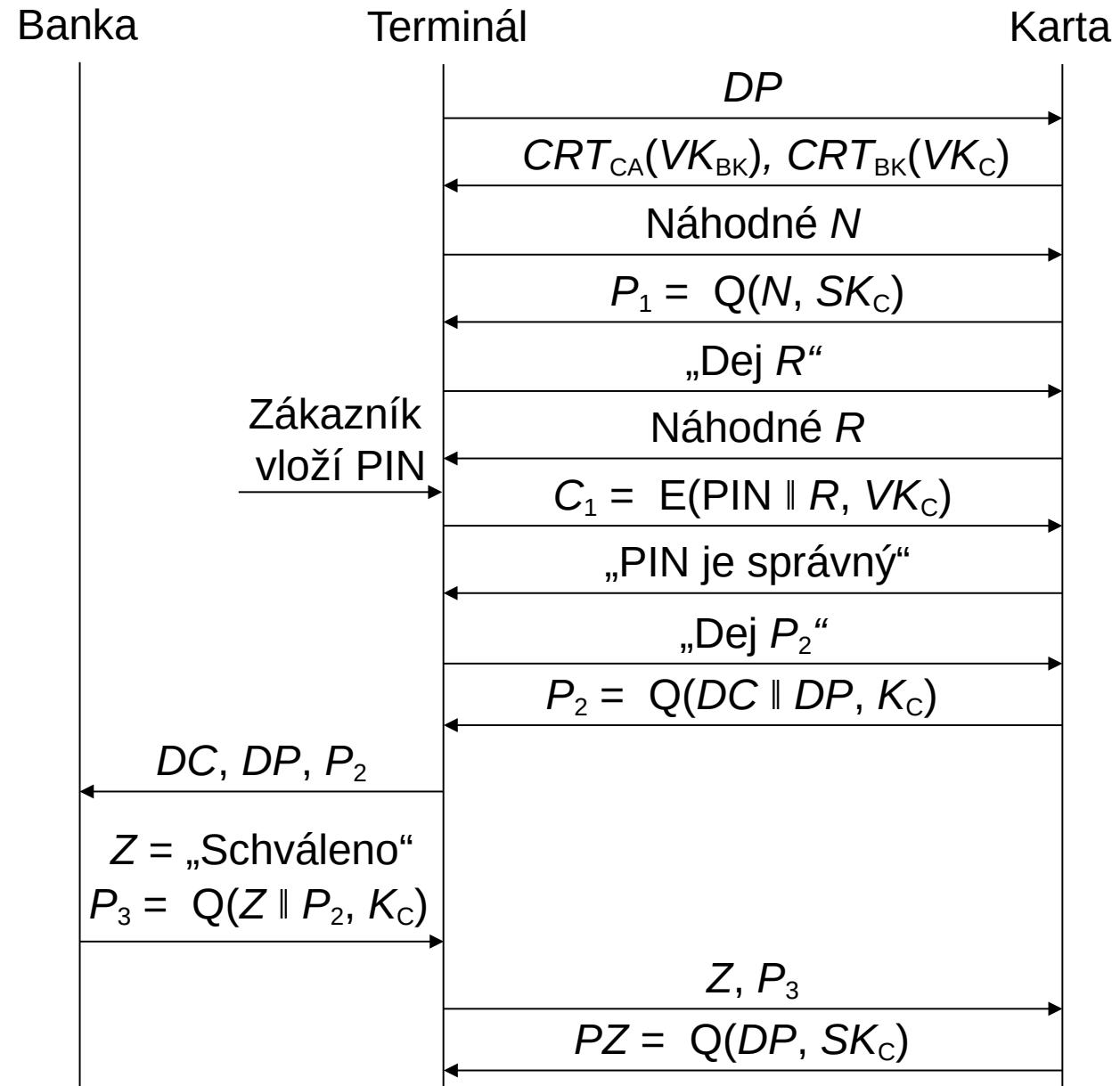
Oběť'



Terminál

Spřažený platební protokol (1/2)

- Spřažený („on-line“) platební protokol je bezpečnější. Vyžaduje však účast banky klienta a proto je používán k platbám většími částkami. Uživatel rovněž v průběhu protokolu vkládá přes terminál svůj PIN, kterým se vůči kartě autentizuje.
- Schéma protokolu je vpravo a jeho popis je na následujícím snímku.



Spřažený platební protokol (1/2)

- První čtyři kroky jsou **stejné** jako v nespřažené variantě.
- Po autentizaci karty si terminál vyžádá od klienta vložení **pinu** a od karty si vyžádá náhodné číslo **R**. Kartě pak odešle kryptogram $C_1 = E(PIN \parallel R, VK_C)$. Karta kryptogram dešifruje, zkонтroluje správnost hodnot PIN i R a terminálu oznámí **správnost** pinu.
- Terminál si následně od karty vyžádá pečet' $P_2 = Q(DC \parallel DP, K_C)$.
- Po přijetí pečeti terminál zašle bance klienta trojici DC, DP, P_2 .
- Banka zkонтroluje **správnost** pečeti a **zarezervuje** částku pro platbu. Terminálu zašle zprávu Z = „Schváleno“ spolu s pečetí $P_3 = Q(Z \parallel P_2, K_C)$.
- Terminál dvojici Z a P_3 **předá** kartě, která **ověří** správnost pečeti. Pokud je vše v pořádku, tak terminálu zašle platební závazek $PZ = Q(DP, SK_C)$.
- Terminál pomocí VK_C platební závazek **ověří** a v kladném případě prodejci **oznámí**, že platba proběhla v pořádku.
- Obchodník si přes svoji banku bude později na základě trojice DC, DP a PZ **nárokovat** platbu od banky klienta.

5. Platby kryptoměnou

Kryptoměna

- Digitální měna je měna, kde **platidlem** nejsou bankovky a mince, ale **data**.
- **Kryptoměna** je digitální měna, jejíž platidla se vytvářejí a mezi osobami převádějí pomocí **kryptografických** technik.
- Existuje celá řada kryptoměn, ale první a nejznámější je tzv. Bitcoin.
- **Bitcoin** (zkráceně BTC nebo XBT) je kryptoměna provozovaná v decentralizované platební síti.
- Bitcoin vznikl v roce 2009 tím, že neznámý **anonym** s přezdívkou Satoshi Nakamoto dal na internetu volně k dispozici **popis** a **software** pro tuto kryptoměnu.
- **Platební síť** Bitcoinu sestává z **uzlů**, které lze klasifikovat na klienty a tzv. těžaře. Síť bitcoinu je **decentralizovaná** a provedení platebního převodu vyžaduje **velký** výpočetní výkon. Důvodem je, aby kryptoměnu nemohl ovládnout jednotlivec, či malá skupina.
- **Klienti** reprezentují jednotlivé účastníky plateb (plátce a příjemce). Vlastnictví bitcoinů je anonymní a vlastnické právo k nim se dokazuje digitálním **podpisem**.
- **Těžaři** zajišťují **převody** bitcoinů mezi klienty a do té doby, než budou získány všechny bitcoiny (maximální počet bitcoinů je uměle nastaven na 21 miliónů), zajišťují i **získávání** nových bitcoinů. Výpočetní obtížnost převodů a získávání bitcoinů je založena na nalezení **heše** s požadovanou vlastností.

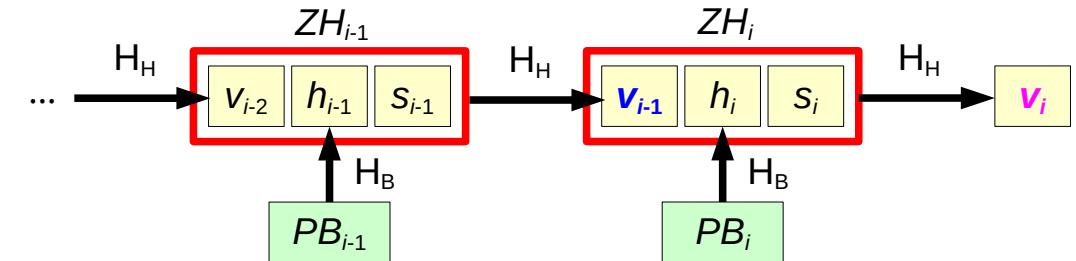
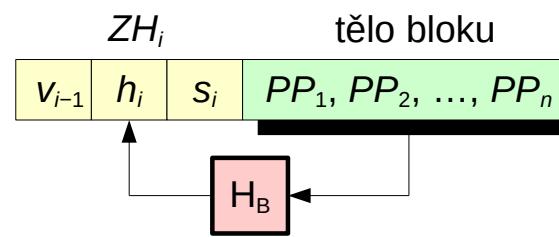


Platební příkaz

- Uživatelé kryptoměny Bitcoin mají obecně více účtů. My však budeme v dalším popisu zjednodušeně předpokládat, že uživatelé mají jen jeden účet.
- Účet uživatele X je dán dvojicí veřejný klíč VK_x a soukromý klíč SK_x podepisovacího kryptosystému. Uživatelé si své účty generují samostatně a anonymně. Síťovým identifikátorem (číslem) účtu je hodnota VK_x .
- Předpokládejme, že uživatel A má na svém účtu VK_A celkem x bitcoinů a chce y bitcoinů převést na účet uživatele B , jehož identifikátorem a zároveň klíčem je VK_B .
- Uživatel A vytvoří platební příkaz (tzv. transakci) PP_{AB} , což je jím podepsaná zpráva, v níž je uvedeno, že ze všech x bitcoinů na účtu VK_A se y bitcoinů převádí na účet VK_B a zbývajících $(x-y)$ bitcoinů se převádí zpět na účet VK_A .
- Platební příkaz musí být podepsán klíčem SK_A , který odpovídá účtu plátce a tedy i identifikátoru a zároveň klíči VK_A . Část převáděných bitcoinů může být předepsána i na odměnu těžaře.
- Všechny dosud provedené platební převody od okamžiku vzniku sítě Bitcoin jsou uloženy v tzv. platební historii, která je známa všem uzlům. Uzly si podle ní kontrolují, že uživatel A skutečně disponuje x bitcoiny a platební příkaz PP_{AB} pak lavinově předávají svým sousedům sítě Bitcoin, aby se příkaz dostal ke všem uzlům sítě. Samotný převod bitcoinů pak provádějí těžaři (viz dále).

Platební převod

- Těžaři doposud neuskutečněné platební příkazy PP seskupují do číslovaných platebních bloků PB . Platební příkazy v těle i -tého bloku PB_i (obr. vlevo) reprezentuje heš $h_i = H_B(PP_1, PP_2, \dots, PP_n)$, kde H_B je funkce určená pro hešování bloků.
- Veškerá platební historie PH (tj. vytvoření nových bitcoinů a jejich převody) se archivuje, přičemž autentičnost všech $(i-1)$ bloků v platební historii (obr. vpravo) chrání heš v_{i-1} .
- Cílem každého těžaře je zřetězit svůj blok PB_i s dosavadní platební historií, která je reprezentována hodnotou v_{i-1} . Získá tím odměnu a zároveň i převede bitcoiny mezi účty podle platebních příkazů v bloku PB_i .
- K uvedenému zřetězení musí těžař nalézt takovou hodnotu s_i (nazveme ji spřáhlo), kdy hodnota $v_i = H_H(ZH_i) < Mx$, přičemž $ZH_i = (v_{i-1} \parallel h_i \parallel s_i)$ je záhlaví bloku PB_i , H_H je stanovená hešovací funkce a práh Mx se mění podle aktuálního výpočetního výkonu sítě.
- Kdo první nalezne spřáhlo, zapojí svůj blok do řetězce platební historie a v něm obsažené platební příkazy tak budou realizovány. Tato informace se lavinově rozšíří po síti. Těžaři si zaktualizují své bloky a od této chvíle se budou snažit připojit své bloky na hodnotu v_i .



6. Závěr

Závěr

- Kryptografické techniky se staly nedílnou součástí zabezpečení moderních elektronických systémů.
- Elektronické platební systémy umožňují rychlé a jednoduché platby. Zároveň však vytvářejí nové hrozby (např. neoprávněné platby apod.).
- Elektronické platební systémy využívají:
 - různé komunikační systémy (internet, GSM, telefonní síť),
 - různé terminály (telefon, PC, platební terminál, bankomat).
- Otázka ke zkoušce:
Elektronické platební systémy:
 - účel,
 - typy a jejich charakteristika,
 - vysvětlit protokol TLS,
 - vysvětlit nespřažený platební protokol.
- Pro zájemce o podrobnější popis fungování kryptografických protokolů:
Burda K.: **Kryptografie okolo nás**. Praha, CZ.NIC 2019.
Volně ke stažení na: <https://knihy.nic.cz/>