Bezpečnost elektronických platebních systémů

Marek Honzírek

Katedra matematiky, Fakulta jaderná a fyzikálně inženýrská,
České vysoké učení technické v Praze

Plán

- Platby kartou na terminálech/bankomaty
- Platby kartou na webu
- Internetové bankovnictví

Platby kartou na terminálech/bankomaty

- bankomaty (ATM terminal)
- Pokladní místa (POS terminal)

Platby kartou na terminálech/bankomaty

MAC funkce: otisk = f(klíč)[text]

Platby kartou na terminálech/bankomaty

- off-line transakce
- on-line transakce
- Terminal risk management
  - Exception file – zablokované karty
  - Výše částky
  - Počet off-line transakcí
  - Náhodně
- ověřování PINu
  - off-line
  - on-line

Platby kartou na terminálech/bankomaty

- off-line transakce
- on-line transakce
- Terminal risk management
  - Exception file – zablokované karty
  - Výše částky
  - Počet off-line transakcí
  - Náhodně
- ověřování PINu
  - off-line
  - on-line

Platby kartou na terminálech/bankomaty

- off-line transakce
- on-line transakce
- Terminal risk management
  - Exception file – zablokované karty
  - Výše částky
  - Počet off-line transakcí
  - Náhodně
- ověřování PINu
  - off-line
  - on-line

Platby kartou na terminálech/bankomaty

- off-line transakce
- on-line transakce
- Terminal risk management
  - Exception file – zablokované karty
  - Výše částky
  - Počet off-line transakcí
  - Náhodně
- ověřování PINu
  - off-line
  - on-line

Platby kartou na terminálech/bankomaty

- off-line transakce
- on-line transakce
- Terminal risk management
  - Exception file – zablokované karty
  - Výše částky
  - Počet off-line transakcí
  - Náhodně
- ověřování PINu
  - off-line
  - on-line

Platby kartou na terminálech/bankomaty

- off-line transakce
- on-line transakce
- Terminal risk management
  - Exception file – zablokované karty
  - Výše částky
  - Počet off-line transakcí
  - Náhodně
- ověřování PINu
  - off-line
  - on-line

Platby kartou na terminálech/bankomaty

- off-line transakce
- on-line transakce
- Terminal risk management
  - Exception file – zablokované karty
  - Výše částky
  - Počet off-line transakcí
  - Náhodně
- ověřování PINu
  - off-line
  - on-line

Platby kartou na terminálech/bankomaty

- off-line transakce
- on-line transakce
- Terminal risk management
  - Exception file – zablokované karty
  - Výše částky
  - Počet off-line transakcí
  - Náhodně
- ověřování PINu
  - off-line
  - on-line

Platby kartou na terminálech/bankomaty

- off-line transakce
- on-line transakce
- Terminal risk management
  - Exception file – zablokované karty
  - Výše částky
  - Počet off-line transakcí
  - Náhodně
- ověřování PINu
  - off-line
  - on-line

Autorizace (ICC) karty off-line

- SAM - obsahuje MK
- výpočet *mac_card*
  - $SSK = F_3(K_d)[ATC]$
  - $mac\_card = F_4(SSK)[M]$
- výpočet *mac_witness*
  - $IMK = F_2(MK)[Issuer\_Identifier]$
  - $K'_d = F_1(IMK)[PAN]$
  - $SSK' = F_3(K'_d)[ATC]$
  - $mac\_witness = F_4(SSK')[M]$
- $mac\_witness \stackrel{?}{=} mac\_card$

Autorizace (ICC) karty off-line

- SAM - obsahuje MK
- výpočet *mac_card*
  - $SSK = F_3(K_d)[ATC]$
  - $mac\_card = F_4(SSK)[M]$
- výpočet *mac_witness*
  - $IMK = F_2(MK)[Issuer\_Identifier]$
  - $K'_d = F_1(IMK)[PAN]$
  - $SSK' = F_3(K'_d)[ATC]$
  - $mac\_witness = F_4(SSK')[M]$
- $mac\_witness \stackrel{?}{=} mac\_card$

Autorizace (ICC) karty off-line

- SAM - obsahuje MK
- výpočet *mac_card*
  - $SSK = F_3(K_d)[ATC]$
  - $mac\_card = F_4(SSK)[M]$
- výpočet *mac_witness*
  - $IMK = F_2(MK)[Issuer\_Identifier]$
  - $K'_d = F_1(IMK)[PAN]$
  - $SSK' = F_3(K'_d)[ATC]$
  - $mac\_witness = F_4(SSK')[M]$
- $mac\_witness \stackrel{?}{=} mac\_card$

Autorizace (ICC) karty off-line

- SAM - obsahuje MK
- výpočet mac_card
  - $SSK = F_3(K_d)[ATC]$
  - $mac\_card = F_4(SSK)[M]$
- výpočet $mac\_witness$
  - $IMK = F_2(MK)[Issuer\_Identifier]$
  - $K'_d = F_1(IMK)[PAN]$
  - $SSK' = F_3(K'_d)[ATC]$
  - $mac\_witness = F_4(SSK')[M]$
- $mac\_witness \stackrel{?}{=} mac\_card$

Autorizace (ICC) karty off-line

- SAM - obsahuje MK
- výpočet *mac_card*
  - $SSK = F_3(K_d)[ATC]$
  - $mac\_card = F_4(SSK)[M]$
- výpočet *mac_witness*
  - $IMK = F_2(MK)[Issuer\_Identifier]$
  - $K'_d = F_1(IMK)[PAN]$
  - $SSK' = F_3(K'_d)[ATC]$
  - $mac\_witness = F_4(SSK')[M]$
- $mac\_witness \stackrel{?}{=} mac\_card$

Autorizace (ICC) karty off-line

- SAM - obsahuje MK
- výpočet mac_card
  - $SSK = F_3(K_d)[ATC]$
  - $mac\_card = F_4(SSK)[M]$
- výpočet $mac\_witness$
  - $IMK = F_2(MK)[Issuer\_Identifier]$
  - $K'_d = F_1(IMK)[PAN]$
  - $SSK' = F_3(K'_d)[ATC]$
  - $mac\_witness = F_4(SSK')[M]$
- $mac\_witness \stackrel{?}{=} mac\_card$

Autorizace (ICC) karty off-line

- SAM - obsahuje MK
- výpočet mac_card
  - $SSK = F_3(K_d)[ATC]$
  - $mac\_card = F_4(SSK)[M]$
- výpočet $mac\_witness$
  - $IMK = F_2(MK)[Issuer\_Identifier]$
  - $K'_d = F_1(IMK)[PAN]$
  - $SSK' = F_3(K'_d)[ATC]$
  - $mac\_witness = F_4(SSK')[M]$
- $mac\_witness \stackrel{?}{=} mac\_card$

Autorizace (ICC) karty off-line

- SAM - obsahuje MK
- výpočet mac_card
  - $SSK = F_3(K_d)[ATC]$
  - $mac\_card = F_4(SSK)[M]$
- výpočet $mac\_witness$
  - $IMK = F_2(MK)[Issuer\_Identifier]$
  - $K'_d = F_1(IMK)[PAN]$
  - $SSK' = F_3(K'_d)[ATC]$
  - $mac\_witness = F_4(SSK')[M]$
- $mac\_witness \stackrel{?}{=} mac\_card$

Autorizace (ICC) karty off-line

- SAM - obsahuje MK
- výpočet mac_card
  - $SSK = F_3(K_d)[ATC]$
  - $mac\_card = F_4(SSK)[M]$
- výpočet $mac\_witness$
  - $IMK = F_2(MK)[Issuer\_Identifier]$
  - $K'_d = F_1(IMK)[PAN]$
  - $SSK' = F_3(K'_d)[ATC]$
  - $mac\_witness = F_4(SSK')[M]$
- $mac\_witness \stackrel{?}{=} mac\_card$

Autorizace (ICC) karty off-line

- SAM - obsahuje MK
- výpočet mac_card
  - $SSK = F_3(K_d)[ATC]$
  - $mac\_card = F_4(SSK)[M]$
- výpočet $mac\_witness$
  - $IMK = F_2(MK)[Issuer\_Identifier]$
  - $K'_d = F_1(IMK)[PAN]$
  - $SSK' = F_3(K'_d)[ATC]$
  - $mac\_witness = F_4(SSK')[M]$
- $mac\_witness \stackrel{?}{=} mac\_card$

Ověřování PINu

- On-line
  - Encrypting PIN Pad (EPP) – 3DES – klíč $TK1$
  - SAM dešifruje a znovu zašifruje klíčem $TK2$ a pošle vydavateli karty
  - vydavatel vypočte PIN image control value a porovná s hodnotou v databázi
- Off-line
  - PIN encryption key – PEK – zná SAM i karta
  - užití symetrického šifrování
  - ICC porovná PIN image control value s PIN image stored value
  - V případě nepřítomnosti PEK lze užít asymetrické šifrování (RSA)

Ověřování PINu

- On-line
  - Encrypting PIN Pad (EPP) – 3DES – klíč $TK1$
  - SAM dešifruje a znovu zašifruje klíčem $TK2$ a pošle vydavateli karty
  - vydavatel vypočte PIN image control value a porovná s hodnotou v databázi
- Off-line
  - PIN encryption key – PEK – zná SAM i karta
  - užití symetrického šifrování
  - ICC porovná PIN image control value s PIN image stored value
  - V případě nepřítomnosti PEK lze užít asymetrické šifrování (RSA)

Ověřování PINu

- On-line
  - Encrypting PIN Pad (EPP) – 3DES – klíč $TK1$
  - SAM dešifruje a znovu zašifruje klíčem $TK2$ a pošle vydavateli karty
  - vydavatel vypočte PIN image control value a porovná s hodnotou v databázi
- Off-line
  - PIN encryption key – PEK – zná SAM i karta
  - užití symetrického šifrování
  - ICC porovná PIN image control value s PIN image stored value
  - V případě nepřítomnosti PEK lze užít asymetrické šifrování (RSA)

Ověřování PINu

- On-line
  - Encrypting PIN Pad (EPP) – 3DES – klíč $TK1$
  - SAM dešifruje a znovu zašifruje klíčem $TK2$ a pošle vydavateli karty
  - vydavatel vypočte PIN image control value a porovná s hodnotou v databázi
- Off-line
  - PIN encryption key – PEK – zná SAM i karta
  - užití symetrického šifrování
  - ICC porovná PIN image control value s PIN image stored value
  - V případě nepřítomnosti PEK lze užít asymetrické šifrování (RSA)

Ověřování PINu

- On-line
  - Encrypting PIN Pad (EPP) – 3DES – klíč $TK1$
  - SAM dešifruje a znovu zašifruje klíčem $TK2$ a pošle vydavateli karty
  - vydavatel vypočte PIN image control value a porovná s hodnotou v databázi
- Off-line
  - PIN encryption key – PEK – zná SAM i karta
  - užití symetrického šifrování
  - ICC porovná PIN image control value s PIN image stored value
  - V případě nepřítomnosti PEK lze užít asymetrické šifrování (RSA)

Ověřování PINu

- On-line
  - Encrypting PIN Pad (EPP) – 3DES – klíč $TK1$
  - SAM dešifruje a znovu zašifruje klíčem $TK2$ a pošle vydavateli karty
  - vydavatel vypočte PIN image control value a porovná s hodnotou v databázi
- Off-line
  - PIN encryption key – PEK – zná SAM i karta
  - užití symetrického šifrování
  - ICC porovná PIN image control value s PIN image stored value
  - V případě nepřítomnosti PEK lze užít asymetrické šifrování (RSA)

Ověřování PINu

- On-line
  - Encrypting PIN Pad (EPP) – 3DES – klíč $TK1$
  - SAM dešifruje a znovu zašifruje klíčem $TK2$ a pošle vydavateli karty
  - vydavatel vypočte PIN image control value a porovná s hodnotou v databázi
- Off-line
  - PIN encryption key – PEK – zná SAM i karta
  - užití symetrického šifrování
  - ICC porovná PIN image control value s PIN image stored value
  - V případě nepřítomnosti PEK lze užít asymetrické šifrování (RSA)

Ověřování PINu

- On-line
  - Encrypting PIN Pad (EPP) – 3DES – klíč $TK1$
  - SAM dešifruje a znovu zašifruje klíčem $TK2$ a pošle vydavateli karty
  - vydavatel vypočte PIN image control value a porovná s hodnotou v databázi
- Off-line
  - PIN encryption key – PEK – zná SAM i karta
  - užití symetrického šifrování
  - ICC porovná PIN image control value s PIN image stored value
  - V případě nepřítomnosti PEK lze užít asymetrické šifrování (RSA)

Ověřování PINu

- On-line
  - Encrypting PIN Pad (EPP) – 3DES – klíč $TK1$
  - SAM dešifruje a znovu zašifruje klíčem $TK2$ a pošle vydavateli karty
  - vydavatel vypočte PIN image control value a porovná s hodnotou v databázi
- Off-line
  - PIN encryption key – PEK – zná SAM i karta
  - užití symetrického šifrování
  - ICC porovná PIN image control value s PIN image stored value
  - V případě nepřítomnosti PEK lze užít asymetrické šifrování (RSA)

Ověřování PINu

- mBank - u ICC vydaných po 2010 ověřování PINu on-line pouze v případě, že PIN zadán 3x po sobě špatně
- Problematická synchronizace PINu na kartě a v bankovním systému

Ověřování PINu

- mBank - u ICC vydaných po 2010 ověřování PINu on-line pouze v případě, že PIN zadán 3x po sobě špatně
- Problematická synchronizace PINu na kartě a v bankovním systému

Platby kartou na webu

- TLS - protokol, poskytnutí zabezpečeného kanálu
- zřízení kanálu – asymetricky (RSA)
- klient povinně ověřuje certifikát serveru pomocí CA
- server volitelně ověřuje certifikát klienta
- komunikace pak šifrována symetricky - DES, RC4, AES (v 1.2)
- integrita komunikace ověřována pomocí hašovacích funkcí - MD5, SHA

Platby kartou na webu

- TLS - protokol, poskytnutí zabezpečeného kanálu
- zřízení kanálu – asymetricky (RSA)
- klient povinně ověřuje certifikát serveru pomocí CA
- server volitelně ověřuje certifikát klienta
- komunikace pak šifrována symetricky - DES, RC4, AES (v 1.2)
- integrita komunikace ověřována pomocí hašovacích funkcí - MD5, SHA

Platby kartou na webu

- TLS - protokol, poskytnutí zabezpečeného kanálu
- zřízení kanálu – asymetricky (RSA)
- klient povinně ověřuje certifikát serveru pomocí CA
- server volitelně ověřuje certifikát klienta
- komunikace pak šifrována symetricky - DES, RC4, AES (v 1.2)
- integrita komunikace ověřována pomocí hašovacích funkcí - MD5, SHA

Platby kartou na webu

- TLS - protokol, poskytnutí zabezpečeného kanálu
- zřízení kanálu – asymetricky (RSA)
- klient povinně ověřuje certifikát serveru pomocí CA
- server volitelně ověřuje certifikát klienta
- komunikace pak šifrována symetricky - DES, RC4, AES (v 1.2)
- integrita komunikace ověřována pomocí hašovacích funkcí - MD5, SHA

Platby kartou na webu

- TLS - protokol, poskytnutí zabezpečeného kanálu
- zřízení kanálu – asymetricky (RSA)
- klient povinně ověřuje certifikát serveru pomocí CA
- server volitelně ověřuje certifikát klienta
- komunikace pak šifrována symetricky - DES, RC4, AES (v 1.2)
- integrita komunikace ověřována pomocí hašovacích funkcí - MD5, SHA

Platby kartou na webu

- TLS - protokol, poskytnutí zabezpečeného kanálu
- zřízení kanálu – asymetricky (RSA)
- klient povinně ověřuje certifikát serveru pomocí CA
- server volitelně ověřuje certifikát klienta
- komunikace pak šifrována symetricky - DES, RC4, AES (v 1.2)
- integrita komunikace ověřována pomocí hašovacích funkcí - MD5, SHA

Nedostatky TLS

- držitel karty může popřít svojí účast na transakci
- data karty uloženy v počítači obchodníka
- snaží se řešit protokol SET
- neprosadil se a byl částečně nahrazen protokolem 3-D Secure
- alternativa – PayPal

Nedostatky TLS

- držitel karty může popřít svojí účast na transakci
- data karty uloženy v počítači obchodníka
- snaží se řešit protokol SET
- neprosadil se a byl částečně nahrazen protokolem 3-D Secure
- alternativa – PayPal

Nedostatky TLS

- držitel karty může popřít svojí účast na transakci
- data karty uloženy v počítači obchodníka
- snaží se řešit protokol SET
- neprosadil se a byl částečně nahrazen protokolem 3-D Secure
- alternativa – PayPal

Nedostatky TLS

- držitel karty může popřít svojí účast na transakci
- data karty uloženy v počítači obchodníka
- snaží se řešit protokol SET
- neprosadil se a byl částečně nahrazen protokolem 3-D Secure
- alternativa – PayPal

Nedostatky TLS

- držitel karty může popřít svojí účast na transakci
- data karty uloženy v počítači obchodníka
- snaží se řešit protokol SET
- neprosadil se a byl částečně nahrazen protokolem 3-D Secure
- alternativa – PayPal

Internetové bankovnictví

- oboustranně ověřená TLS komunikace
- certifikát v souboru (soft token)
- certifikát na čipové kartě (hardware token)
- Jednorázové heslo – SMS

Internetové bankovnictví

- oboustranně ověřená TLS komunikace
- certifikát v souboru (soft token)
- certifikát na čipové kartě (hardware token)
- Jednorázové heslo – SMS

Internetové bankovnictví

- oboustranně ověřená TLS komunikace
- certifikát v souboru (soft token)
- certifikát na čipové kartě (hardware token)
- Jednorázové heslo – SMS

Internetové bankovnictví

- oboustranně ověřená TLS komunikace
- certifikát v souboru (soft token)
- certifikát na čipové kartě (hardware token)
- Jednorázové heslo – SMS

Literatura

- Cristian Radu, *Implementing Electronic Card Payment Systems*, Artech House, Inc., 2003.
- A. Hiltgen, T. Kramp and T. Weigold, *Secure Internet Banking Authentication*, The IEEE Computer Society, 2005
- www.mesec.cz
- www.mbank.cz
- www.wikipedia.org