Správa revokovaných certifikátů v elektronickém platebním systému

Vít Bukač, Roman Žilka, Andriy Stetsko
Fakulta informatiky
Masarykova univerzita

Osnova

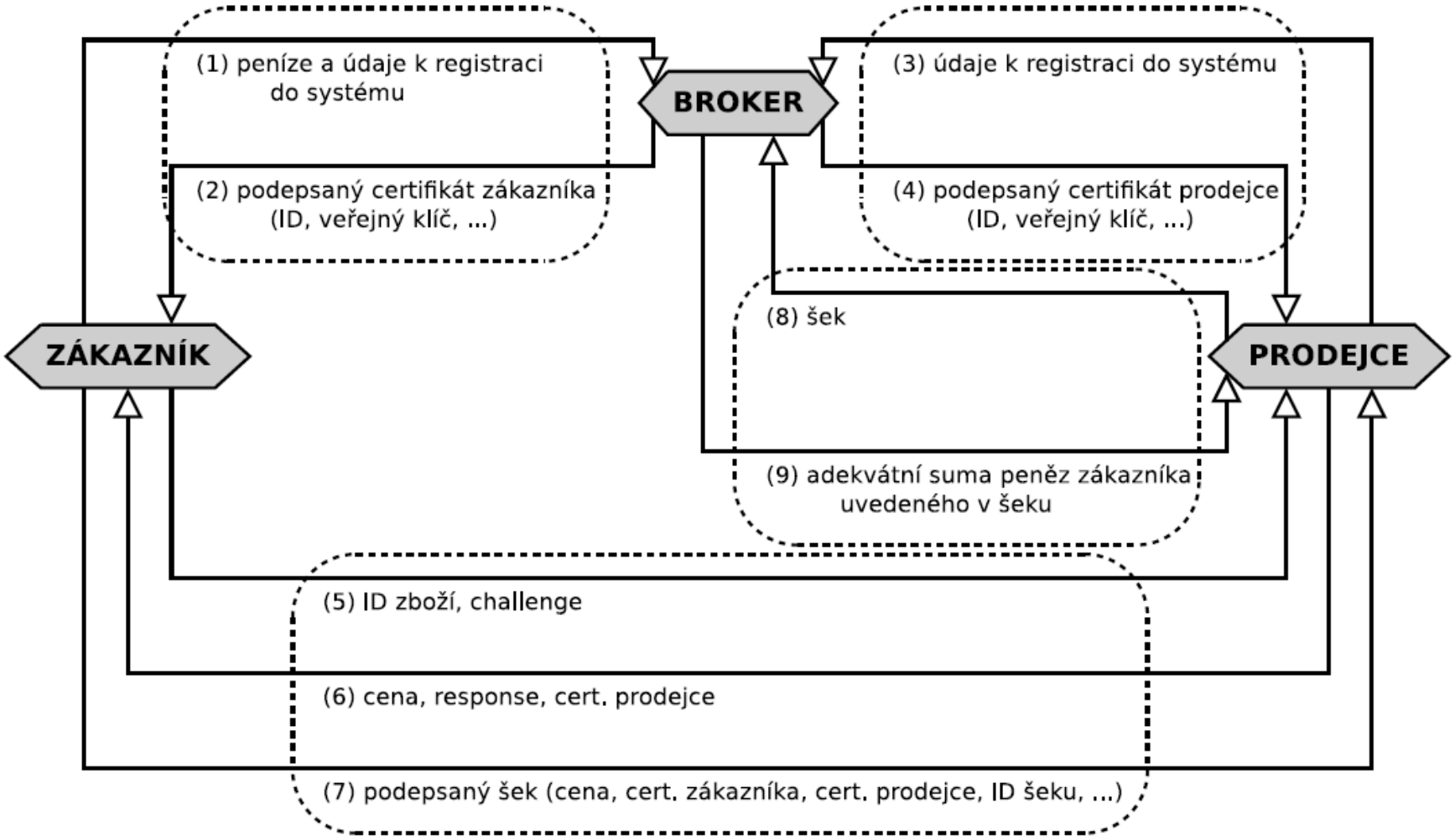
- Mikroplatební schéma
- Metody ověření certifikátu
- Je možné provozovat revokační služby na běžně dostupném hardwaru?

Mikroplatební schéma

Základní fakta

- Nízkonákladové nákupy čipovou kartou
- Role
  - Broker
  - Prodejce
  - Zákazník

Schéma


(1) peníze a údaje k registraci do systému
BROKER
(3) údaje k registraci do systému
(2) podepsaný certifikát zákazníka (ID, veřejný klíč, ...)
(4) podepsaný certifikát prodejce (ID, veřejný klíč, ...)
(8) šek
ZÁKAZNÍK
PRODEJCE
(9) adekvátní suma peněz zákazníka uvedeného v šeku
(5) ID zboží, challenge
(6) cena, response, cert. prodejce
(7) podepsaný šek (cena, cert. zákazníka, cert. prodejce, ID šeku, ...)

Důvody revokace

- Zákazník nedodržuje pravidla používání systému
- Je rozvázána smlouva mezi brokerem a zákazníkem
- Zákazník utratí více peněz než kolik svěřil brokerovi do opatrování
- Explicitní zákazníkova žádost (např. ztráta karty)

Metody ověření certifikátu

Strategie přijetí certifikátu

- Liberální
- Konzervativní

CRL

- Certificate revocation list
- Seznam všech revokovaných certifikátů
- Digitálně podepsaná datová struktura
  - Číslo verze
  - Název vydávající CA
  - Datum a čas zveřejnění
  - Datum a čas skončení platnosti
  - Sériová čísla revokovaných certifikátů
  - Datum a čas revokace každého certifikátu

CRL

- Modus operandi
- Režim
  - Push
  - Pull
  - Hybrid

Delta CRL

- Seznam certifikátů, které byly revokovány od vydání posledního CRL
- Typ
  - Rozdílový
  - Inkrementální

OCSP

- Online Certificate Status Protocol
- Protokol typu výzva – odpověď
- Ověřuje pouze revokační status, ne celkovou platnost certifikátu
- Certifikační autorita musí být neustále online

Je možné provozovat revokační služby na běžně dostupném hardwaru?

Testovací situace

- Velikost
  - Plného CRL = 300 KB (~8000 cert.)
  - DeltaCRL15 = 1 KB
  - DeltaCRL120 = 6 KB
  - OCSP zpráva = 250 B
- Každý prodejce obsluhuje 500 zákazníků
- Každý zákazník provádí 10 transakcí denně

Scénáře

	Max. čas chybné přijetí	Max. počet špiček za den
CRL15	15 min	≤ 100
CRL120	2 h	≤ 12
CRL1440	24 h	≤ 1
CRL240+15	15 min	≤ 6
CRL1440+15	15 min	≤ 1
CRL1440+120	2 h	≤ 1
OCSP	0 min	Variabilní

Technologie přenosu

	Datový tok	Technologie	Čas	Latence
Minimální	0 – 1 KB/s			
Velmi malý	1 – 10 KB/s	Dialup	60 s	∼100 ms
		GPRS	40 s	100 ms – 1 s
Malý	10 – 100 KB/s	EDGE	15 s	100 ms – 1 s
Střední	100 KB/s – 1 MB/s	802.11b	1 s	10 – 100 ms
		CDMA	1 s	∼100 ms
		HSDPA	1 s	∼100 ms
Velký	1 – 10 MB/s	802.11a/g/n	1 s	10 – 100 ms
		ADSL	1 s	∼10 ms
		Ethernet	1 s	∼10 ms
Velmi velký	10 – 100 MB/s	Fast Ethernet	1 s	∼10 ms
Extrémní	> 100 MB/s	Gbit Ethernet	1 s	∼1 ms

Nárok na přenosové pásmo brokera

Průměr	< 100 prodejců	100 – 1000 prodejců	> 1000 prodejců
CRL15	Malý	Střední	Střední+
CRL120	Velmi malý	Malý	Malý+
CRL1440	Minimální	Velmi malý	Velmi malý+
CRL240+15	Velmi malý	Malý	Malý+
CRL1440+15	Minimální	Velmi malý	Velmi malý+
CRL1440+120	Minimální	Velmi malý	Velmi malý+
OCSP	Velmi malý	Malý	Malý+

Max	< 100 prodejců	100 – 1000 prodejců	> 1000 prodejců
CRL	Velký	Velmi velký	Velmi velký+
OCSP	Malý	Střední	Střední+

Data stažená prodejcem

	1 h	4 h	1 den
CRL15	1,2 MB	4,8 MB	28,8 MB
CRL120	—	0,6 MB	3,6 MB
CRL1440	—	—	0,3 MB
CRL240+15	—	0,32 MB	2 MB
CRL1440+15	—	—	0,4 MB
CRL1440+120	—	—	0,4 MB
OCSP	0,05 MB	0,2 MB	1,2 MB

Počet kryptooperací brokera/den

	< 100 prodejců	$100 - 1000$ prodejců	> 1000 prodejců
CRL15	< 100	< 100	< 100
CRL120	12	12	12
CRL1440	1	1	1
CRL240+15	< 100	< 100	< 100
CRL1440+15	< 100	< 100	< 100
CRL1440+120	12	12	12
OCSP	500000	5000000	> 5000000

Závěr

- Požadavky na revokační systém závisí na konkrétní situaci
- Běžně dostupný HW je dostatečný i pro brokera

Děkuji za pozornost