GOPAS POCITACOVA.SKOLA.CZ | DAQUAS | Microsoft

TECHNICAL EDUCATION & DEVELOPER DATABASE CONFERENCE 2013

Bezpečné API
Jak to dělat správně

Michal A. Valášek

Microsoft MVP Most Valuable Professional

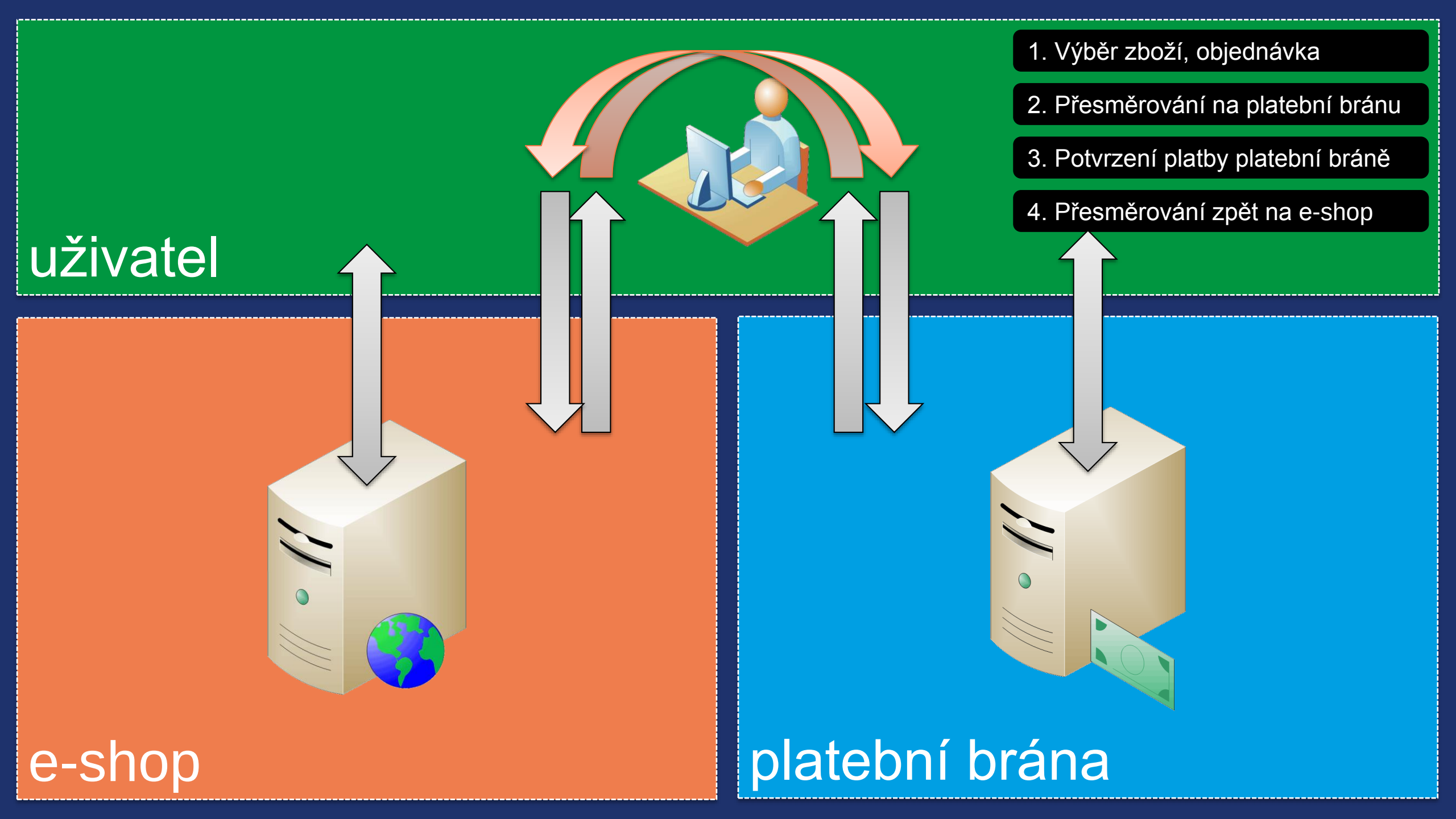
altairis

11. ročník největší odborné IT konference v ČR!

Tech·Ed DevCon Praha 2013

Bezpečné API

- Propojení dvou webových služeb
  - Např. e-shop a platební brána
  - Realizováno nebezpečným kanálem, typicky přes klienta – zákazníka
- Zprávy nutno zabezpečit proti zneužití, zejména:
  - Modifikace dat v průběhu přenosu
  - Replay attack


1. Výběr zboží, objednávka
2. Přesměrování na platební bránu
3. Potvrzení platby platební bráně
4. Přesměrování zpět na e-shop
uživatel
e-shop
platební brána

Přístup naivní

- Zabezpečení žádné nebo statickým heslem
  - Nezáleží příliš na tom, zda je komunikace přímá, nebo přes uživatele!
  - Nevyužívá žádnou kryptografii
- Nejjednodušší řešení
- Útok triviální (komunikace přes uživatele) nebo snadný (komunikace přímo, bez autentizace)

Naivní přístup

demo

Přístup symetrický

- Data jsou zajištěna elektronickým podpisem
- Založeno na sdíleném klíči (HMAC)
- Jednoduchá implementace
  - Stačí umět hashovat (MD5, SHA-1, SHA-2…)
- Z hlediska útoku uživatele bezpečné
- Ale neexistuje nepopiratelnost

Hash Message Authentication Code

- HMAC = „hashování se solí“
  - K datům se přidá tajný klíč (sůl) a zahashuje se to dohromady
- Nejjednodušší forma digitálního podpisu
  - Jenom jako ochrana proti manipulaci z vnějšku
  - Nelze prokázat identitu podepisující osoby
- Bezpečnost HMAC nezávisí na bezpečnosti hashovacího algoritmu, lze použít např. i MD5

Symetrický přístup

demo

Přístup asymetrický

- Pro podpis použijeme RSA klíče
  - Obecně lze použít self-signed certifikáty
  - Opravdový elektronický podpis
- Vyšší náročnost implementace
- Nejbezpečnější varianta
  - Nelze podvrhnout ze strany uživatele
  - Nepopiratelnost protistranou
  - Ovšem pouze v případě, že je obdržena odpověď

Možné problémy

- Bezpečná úschova soukromých klíčů
- Verzování klíčů
- Formát dat (použijte PKCS#7/CMS)
- Obecně nelze použít metodu GET
  - Data jsou příliš dlouhá
  - Použijte POST a skripty
  - Nemá vliv na bezpečnost!

Asymetrický přístup

demo

Problémy, které jsme neřešili

- Některé aspekty replay attacků
  - Typicky se ošetřuje na straně brány
- Obrana proti phishingu
  - Použít SSL a inteligenci uživatele, je-li k dispozici
- Komunikace platební brány s uživatelem
  - To je její problém

dotazy ?

www.aspnet.cz

www.rider.cz

facebook.com/rider.cz

twitter.com/ridercz

ask.fm/ridercz