EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Název projektu	**Rozvoj vzdělávání na Slezské univerzitě v Opavě**
Registrační číslo projektu	**CZ.02.2.69/0.0./0.0/16_015/0002400**

Prezentace předmětu:
Podnikání na Internetu

Vyučující:
doc. Mgr. Petr Suchánek, Ph.D.

SLEZSKÁ UNIVERZITA
OBCHODNĚ PODNIKATELSKÁ FAKULTA V KARVINÉ

Podnikání na Internetu

Přednáška 9

SLEZSKÁ
UNIVERZITA
OBCHODNĚ PODNIKATELSKÁ
FAKULTA V KARVINÉ

doc. Mgr. Petr Suchánek, Ph.D.

Bezpečnost e-business

- Bezpečnost – jedna z klíčových podmínek úspěšnosti
- Původně byla bezpečnost jedna ze základních bariér rozvoje e-business ze strany zákazníků.
- Bezpečnost lze kategorizovat na
  - vnitřní – možné útoky ve vnějším prostředí podniku;
  - vnější – možné útoky z vnějšího prostředí.
- Bezpečnost e-business je úzce vázána na zásady bezpečného chování uživatelů na Internetu:
  - http://www.bezpecnyinternet.cz/

Bezpečnost e-business – digitální podpis

- Dle zákona č. 227/2000 o elektronickém podpisu je elektronický podpis definován jako: Elektronickým podpisem se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě.
- Digitální podpis je spojením klasického elektronického podpisu s certifikátem zajišťujícím identitu člověka.
- Je nutné uvést, že digitální podpis sám o sobě nepotvrzuje identitu uživatele nebo systému. Ta je garantována důvěryhodnou třetí stranou - certifikační autoritou. Vydává důvěryhodný certifikát uživateli na základě znalosti jeho identity.

Bezpečnost e-business – digitální podpis

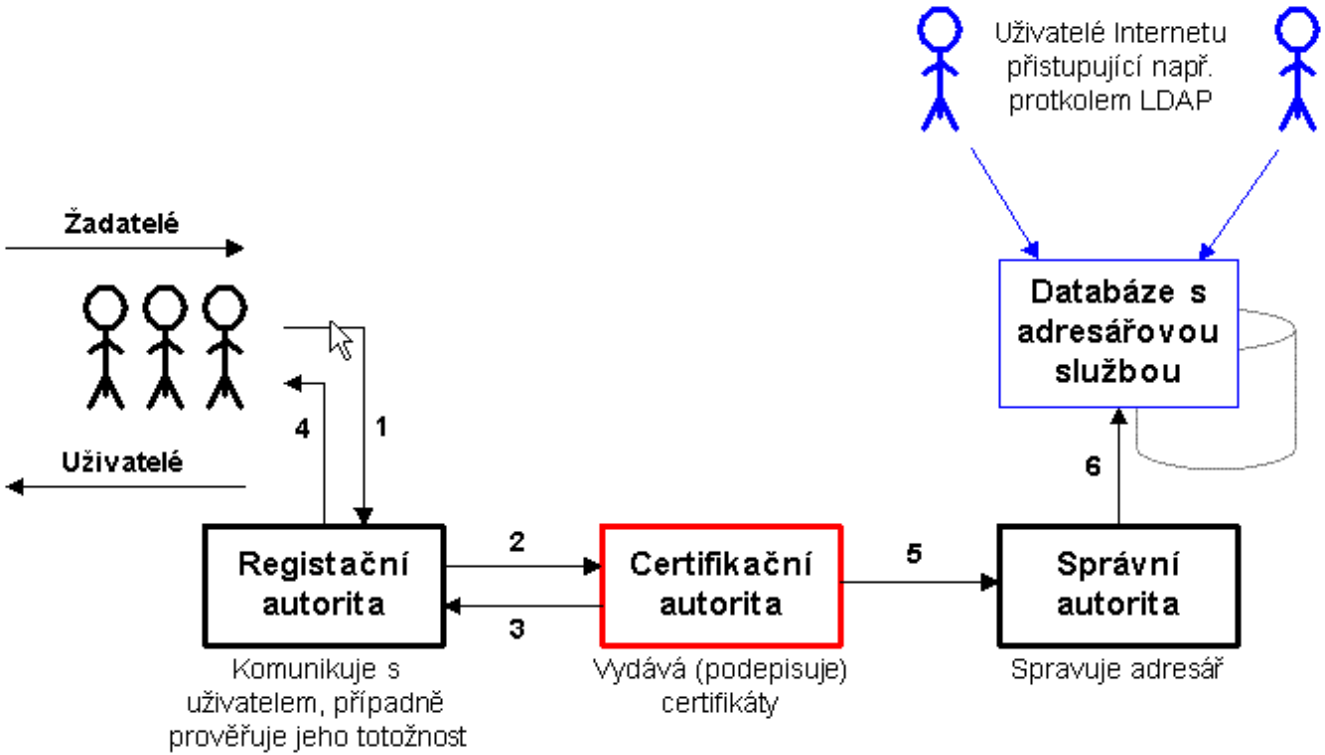
- Certifikační autorita
  - subjekt, který vydává digitální certifikáty (elektronicky podepsané veřejné šifrovací klíče), čímž usnadňuje využívání PKI (Public Key Infrastructure) tak, že svojí autoritou potvrzuje pravdivost údajů, které jsou ve volně dostupném veřejném klíči uvedeny.

Bezpečnost e-business – digitální podpis

- Majitel veřejného klíče musí při žádosti o vydání digitálního certifikátu důvěryhodným způsobem certifikační autoritu přesvědčit, že jím poskytnuté údaje odpovídají skutečnosti a tomu, co uvedl ve svém veřejném klíči.
- CA se skládá za tří základních částí:
  - registrační authority;
  - certifikační authority;
  - správní autority.

Bezpečnost e-business – digitální podpis

SLEZSKÁ UNIVERZITA
OBCHODNĚ PODNIKATELSKÁ FAKULTA V KARVINÉ



http://www.uiam.mtf.stuba.sk/predmety/ps/Cd-II/CD-ca/ca5.htm

Bezpečnost e-business – digitální podpis

- V České republice jsou akreditovány 3 certifikační autority. Jedná se o:
  - První certifikační autorita, a.s., akreditace udělena 15.03.2002;
  - Česká pošta, s.p., akreditace udělena 15.07.2005;
  - eIdentity, a.s., akreditace udělena 12.09.2005;
- Akreditaci pro vydávání kvalifikovaných certifikátů uděluje Ministerstvo vnitra ČR.
- Akreditované certifikační autority mají právo vydávat tyto typy certifikátů:
  - Kvalifikovaný digitální certifikát; - Kvalifikované časové razítko.
  - Kvalifikovaný systémový certifikát;

Bezpečnost e-business – digitální podpis

Pojem	Charakteristika
Kryptologie	Věda o šifrování (je v ní obsažena kryptografie a kryptoanalýza).
Kryptografie	Zabývá se metodami šifrování dat.
Kryptoanalýza	Zabývá se metodami umožňujícími šifrované zprávy neautorizovaně dešifrovat.
Šifrování	Proces, při kterém dochází k převedení obecně srozumitelného textu na zašifrovaný text (jeho obsah nelze přímo určit).
Dešifrování	Proces opačný k šifrování.
Otevřený text	Původní nezašifrovaný text.
Šifrovaný text (šifra)	Zašifrovaný text
Šifrovací (dešifrovací) algoritmus	Funkce, obecně sestavená na matematickém základě, podle které se provádí vlastní šifrování a dešifrování zpráv.
Šifrovací klíč	Binární informace, která slouží jako jednoznačný podmíněný vstupní parametr při šifrování a dešifrování zpráv. Obecně má předem určený počet bitů.

Bezpečnost e-business – digitální podpis

- Jestliže označíme C jako šifru, P otevřený původní text, E (D) šifrovací (dešifrovací) algoritmus a K klíč, pak můžeme šifru obecně vyjádřit jako funkci ve tvaru:

$$C = E(P) \text{ resp. } C = E(K, P) \text{ - šifrování}$$

$$P = D(C) \text{ resp. } P = D(K, C) \text{ - dešifrování}$$

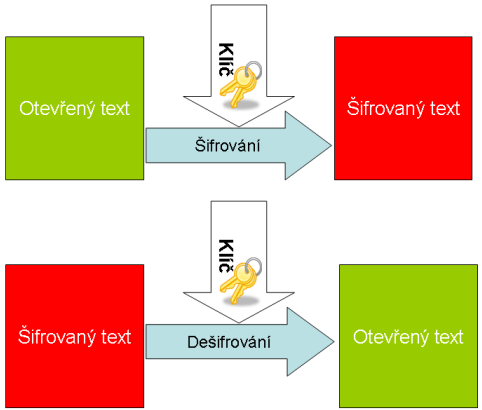
přičemž musí platit, že $P = D(E(P))$

Bezpečnost e-business – digitální podpis

- Zprávy by se zašifrováním neměly zvětšovat.
- Algoritmus šifrování musí čím jak nejvíce zamezit možnosti prolomení šifry, nicméně jeho implementace by měla být co nejjednodušší.
- Algoritmus by v žádném případě neměl být omezující (např. počet znaků a typy znaků).
- Množství práce vynaložené na šifrování a dešifrování by mělo být úměrné požadovanému stupni utajení.
- Chyby při šifrování by se neměly příliš šířit a ovlivňovat následující komunikaci.

Bezpečnost e-business – digitální podpis

- Šifrovací klíč
  - jeden z nejdůležitějších prvků, od kterého se odvíjí bezpečnost šifrovacího systému z hlediska přenosu zašifrovaných dat;
  - prakticky všechny jeho parametry a stadia od generace přes distribuci až po délku platnosti jsou velice důležité;
  - klíč můžeme do jisté míry považovat za jakési "vstupní heslo" šifrovacího (dešifrovacího) algoritmu.

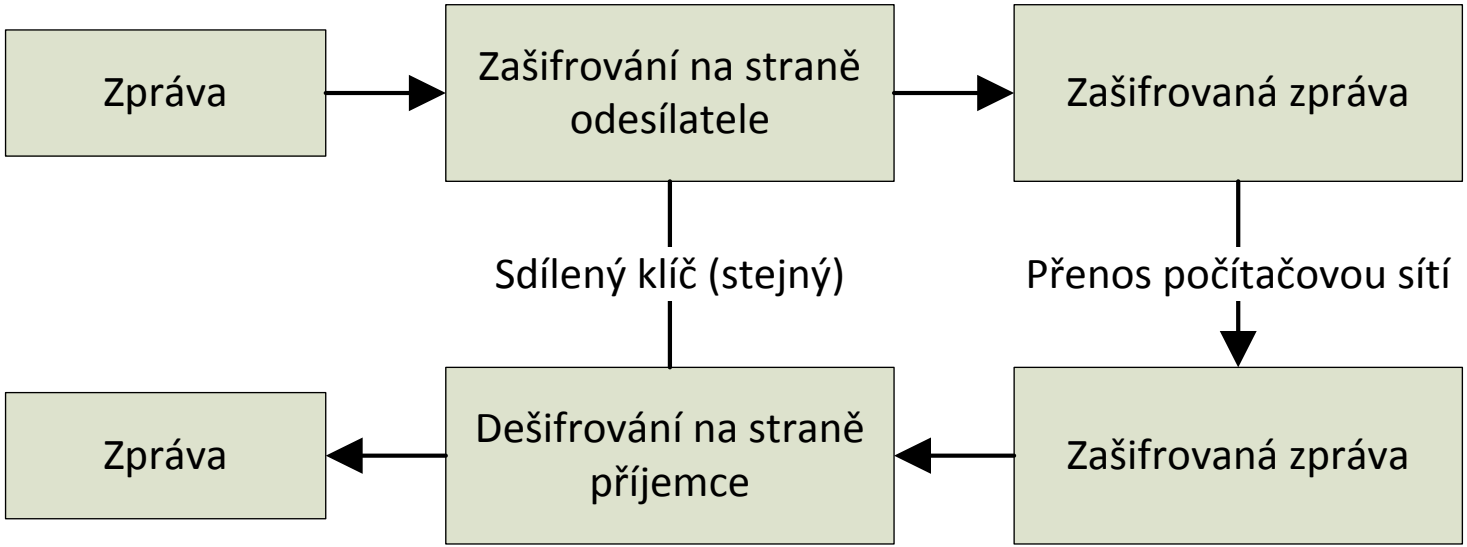


https://cs.wikipedia.org/wiki/Symetrick%C3%A1_%C5%A1ifra

Bezpečnost e-business – digitální podpis

SLEZSKÁ UNIVERZITA
OBCHODNĚ PODNIKATELSKÁ FAKULTA V KARVINÉ

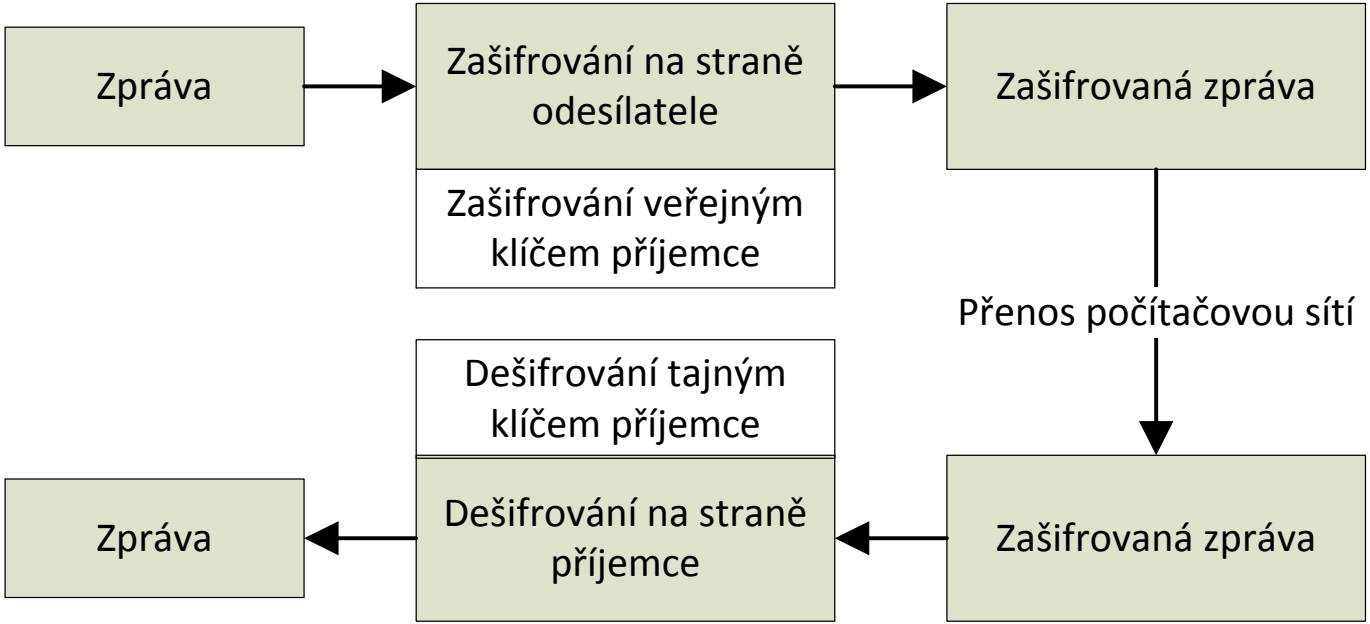
- Šifrování s tajným klíčem



Bezpečnost e-business – digitální podpis

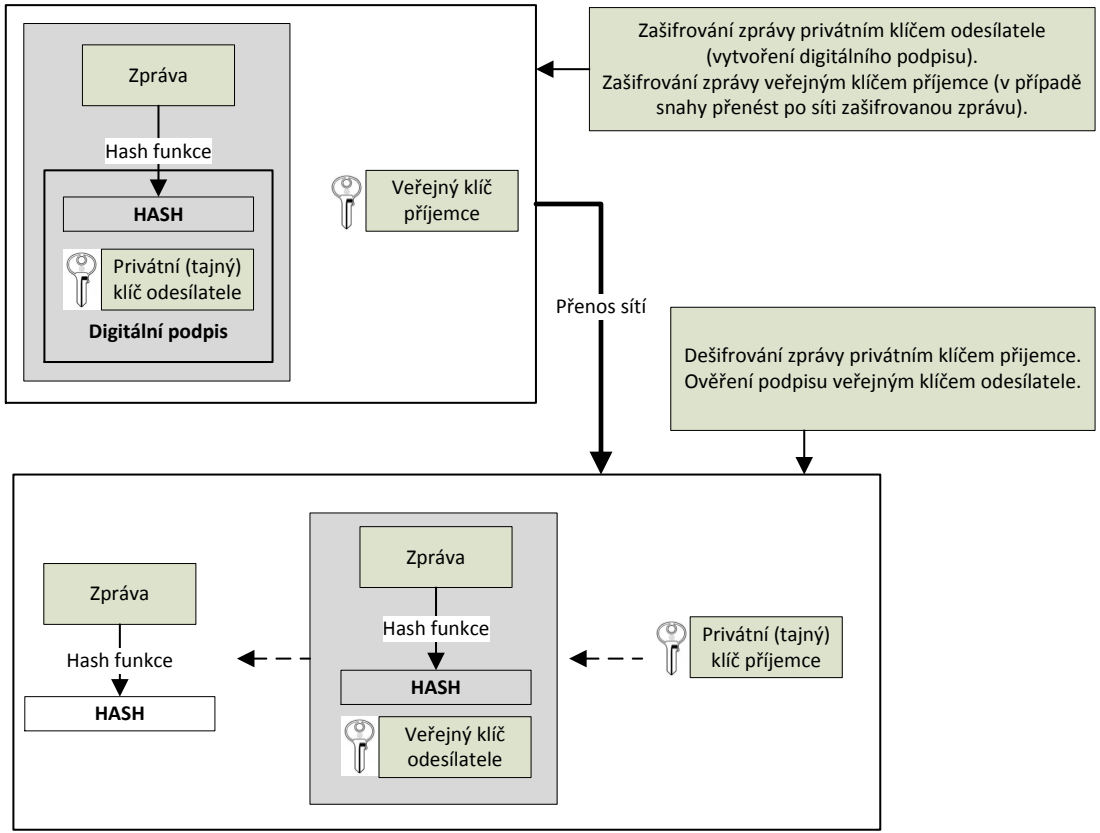
SLEZSKÁ UNIVERZITA
OBCHODNĚ PODNIKATELSKÁ FAKULTA V KARVINÉ

- Šifrování s veřejným klíčem



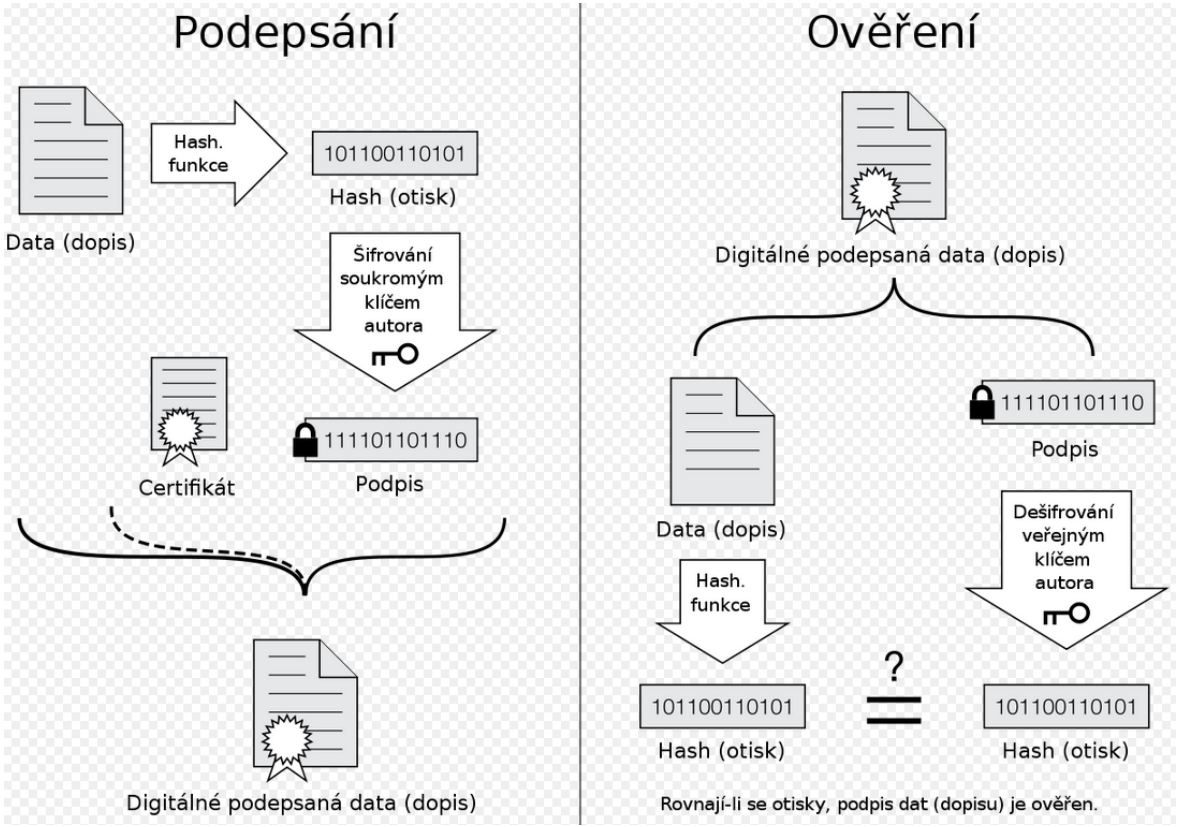
Bezpečnost e-business – digitální podpis

SLEZSKÁ UNIVERZITA
OBCHODNĚ PODNIKATELSKÁ FAKULTA V KARVINÉ



Bezpečnost e-business – digitální podpis

SLEZSKÁ UNIVERZITA
OBCHODNĚ PODNIKATELSKÁ FAKULTA V KARVINÉ



https://cs.wikipedia.org/wiki/Elektronick%C3%BD_podpis#/media/File:Digital_Signature_diagram_cs.svg

Bezpečnost e-business – digitální podpis

- Autentičnost podepisující osoby
  - zprávu mohl podepsat pouze ten, kdo má k deklarovanému veřejnému klíči odpovídající privátní klíč.
- Integritu zprávy
  - v době, která uplynula mezi podepsáním zprávy a ověřováním podpisu, nebyla tato zpráva modifikována.
- Neodmítnutelnost odpovědnosti
  - osoba, která tuto zprávu podepsala, nemůže svou činnost popřít, neboť její znalost privátního klíče je unikátní.
- Časové ukotvení
  - Elektronický podpis může obsahovat časové razítko, které prokazuje datum a čas podepsání dokumentu.

Děkuji za pozornost

Otázky?