Elektronický podpis

Elektronický podpis

- ***Bezpečnost a kryptologie***
- Výměna informací v elektronické podobě je trendem dnešní doby. Ne každá informace je však určená očím a uším každého. Jinak řečeno, data je často třeba chránit.
  S mezinárodními normami (**ITSEC** (**Information Technology Security Evaluation Criteria**) a **ITSEM - … Manual**) můžeme definovat základní bezpečnostní cíle, jejichž plnění by měl důvěryhodný systém zajistit.

Elektronický podpis

- ***důvěrnosti dat***, což znamená, že informace ve výpočetním a přenosovém systému je přístupná pouze pro autorizované subjekty. Přístupem se rozumí zobrazování obsahu, odhalením místa uložení, možností provádět kopie, tisky apod.
- ***autenticity dat***, což znamená, že lze ověřit původ informace (zprávy, elektronického dokumentu apod.)
- ***celistvosti (integrity) dat***, což znamená, že pouze oprávněné subjekty mohou nakládat s aktivy systému (např. manipulovat s daty, přenášet je, oprávněně odpovídat na poštovní zprávy, měnit konfigurace systému apod.)
- ***neodmítnutelné odpovědnosti***, což znamená, že ani zdroj informace (odesílatel dat) ani její cíl (příjemce dat) nemohou popřít svou účast na průběhu výměny této informace (např. před nezávislou třetí stranou)

Elektronický podpis

Jak bezpečného stavu dosáhnout

- Fyzická ochrana
  - Často náročná, většinou nemožná (jak chránit několik kilometrů dlouhé linky proti odposlechu apod.)
- Logická ochrana (šifrování)
  - Věda o šifrování – kryptologie – dva směry
    - **Kryptografie (tvorba šifer)**
    - **Kryptoanalýza (luštění šifer)**

Elektronický podpis

- ***Kódování a šifrování***
- Šifrování se často zaměňuje s pojmem kódování. Není divu, kódování je také proces převodu informace z jedné formy do druhé. Kódování k tomu ale nepoužívá žádnou utajovanou informaci. Proces zakódování a dekódování je zcela veřejný a může ho provést každý. Typickým příkladem jsou kódy ASCII, Latin 2 apod.
- U šifrování, šifrovacího algoritmu ale vždy existuje “něco tajného” - například klíč. Klíč je pak v tomto smyslu tajná náhodná posloupnost bitů, znaků o různé délce. Délka klíče je dána rozumným poměrem mezi bezpečností šifrování a délky procesu šifrovaní.

Elektronický podpis

- Šifrování patří mezi kryptografické bezpečnostní mechanismy, které jsou primárně používány jako ochrana proti ztrátě důvěrnosti informace. Současně lze pomocí šifrování také zajistit autenticitu informace. Šifrování je proces, při kterém se data transformují do formátu, který nemůže být srozumitelný bez zpětné transformace. Z původního "srozumitelného" textu se šifrováním stává "nesrozumitelná" šifra, která může být přenášena ze zdrojového systému přes nezabezpečený přenosový systém (např. přes Internet) do cílového systému. V cílovém systému proběhne dešifrování, při kterém se šifra transformuje do původního textu.

Elektronický podpis

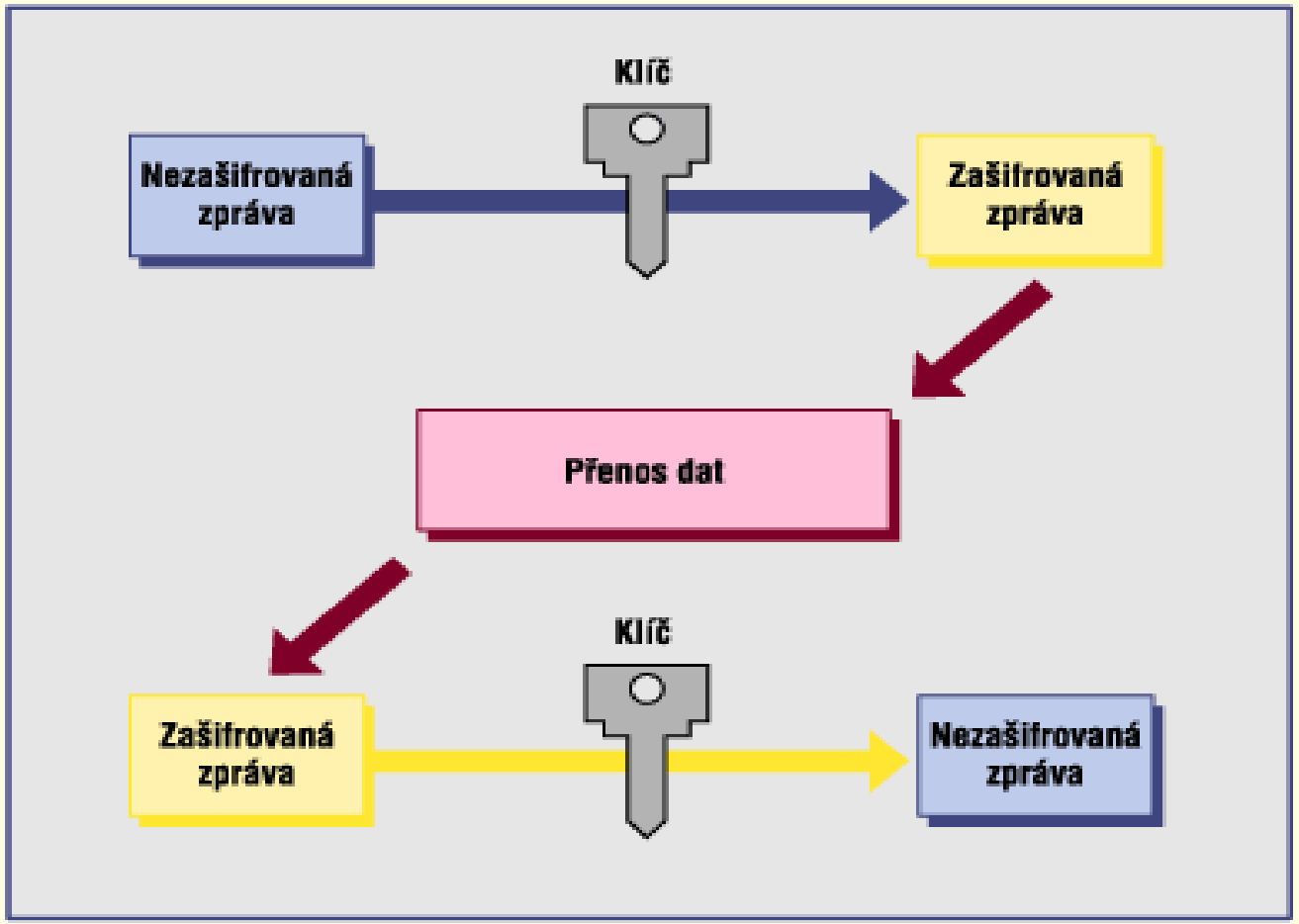
Šifrování a dešifrování se provádí dohodnutým způsobem, který představuje ***šifrovací algoritmus***. Šifrovací algoritmy používají k transformaci textu stanovené parametrické elementy, ***šifrovací klíče*** . Z hlediska programátora se jedná o bitovou sekvenci určité délky (např. 128 bitů, 512 bitů atd.). Délka šifrovací klíče zpravidla určuje "sílu" šifrovacího algoritmu, tj. odolnost proti rozluštění šifry.

Elektronický podpis

- Způsob používání šifrovacího klíče určuje typ šifrovacího algoritmu
  - obě komunikující strany používají stejný klíč pro šifrování a dešifrování, příslušný šifrovací algoritmus náleží do skupiny ***symetrických šifrovacích (kryptografických) algoritmů*** . Společný klíč se nazývá ***tajný klíč (secret key)*** a obě strany jej musí uchovávat v zájmu důvěrnosti sdílených dat v tajnosti před nepovolanou "třetí stranou".

Elektronický podpis

Symetrický algoritmus



Elektronický podpis

Z toho vyplývá nutnost před začátkem komunikace předat důvěryhodným kanálem šifrovací klíč spolu s dalšími údaji (konkrétní typ algoritmu) druhé straně.

Současná komerčně dostupná výpočetní technika aplikuje tyto algoritmy (např. DES (Data Encryption Standard) , TRIPLEDES, IDEA (International Data Encryption Algorithm), RC2 a RC4 (Rivest Cipher).) téměř v reálnem čase. Na druhé straně i nejmodernější výpočetní technika je schopna dešifrovat data bez znalosti příslušných klíčů jen za relativně dlouhé časové období a s velkými finančními náklady. Pomocí matematických metod lze poměrně přesně vyčíslit náklady a čas potřebný k dešifrování dat, které jsou šifrovány definovaným algoritmem. Volbou délky klíče lze navíc tento výsledek výrazně ovlivnit.

Elektronický podpis

Použití symetrických algoritmů představuje způsob, jak zabezpečit důvěrnost transakcí definovaným způsobem s možností přesného stanovení hrozeb, kterým toto zabezpečení odolává.Tyto algoritmy však neřeší důležitý požadavek neodmítnutelnosti odpovědnosti. Nelze totiž určit, která strana zprávu odeslala a která přijala.

Elektronický podpis

Jestliže se klíč používaný jednou stranou pro šifrování liší od klíče používaného druhou stranou pro dešifrování, příslušný šifrovací algoritmus náleží do skupiny ***asymetrických šifrovacích (kryptografických) algoritmů*** . ***Klíč soukromý (private key)***, který v tajnosti uchovává jeho majitel, a ***klíč veřejný (public key)***, který poskytuje k použití svým partnerům, tvoří komplementární dvojici. To znamená, že původní text, který odesilatel šifruje svým soukromým klíčem, je možno dešifrovat pouze jeho příslušným klíčem veřejným. Přenášená data nemají chráněnu důvěrnost, neboť veřejný klíč může používat kdokoliv, avšak u dat je zajištěna autenticita, neboť šifru mohl vygenerovat pouze vlastník příslušného soukromého klíče.

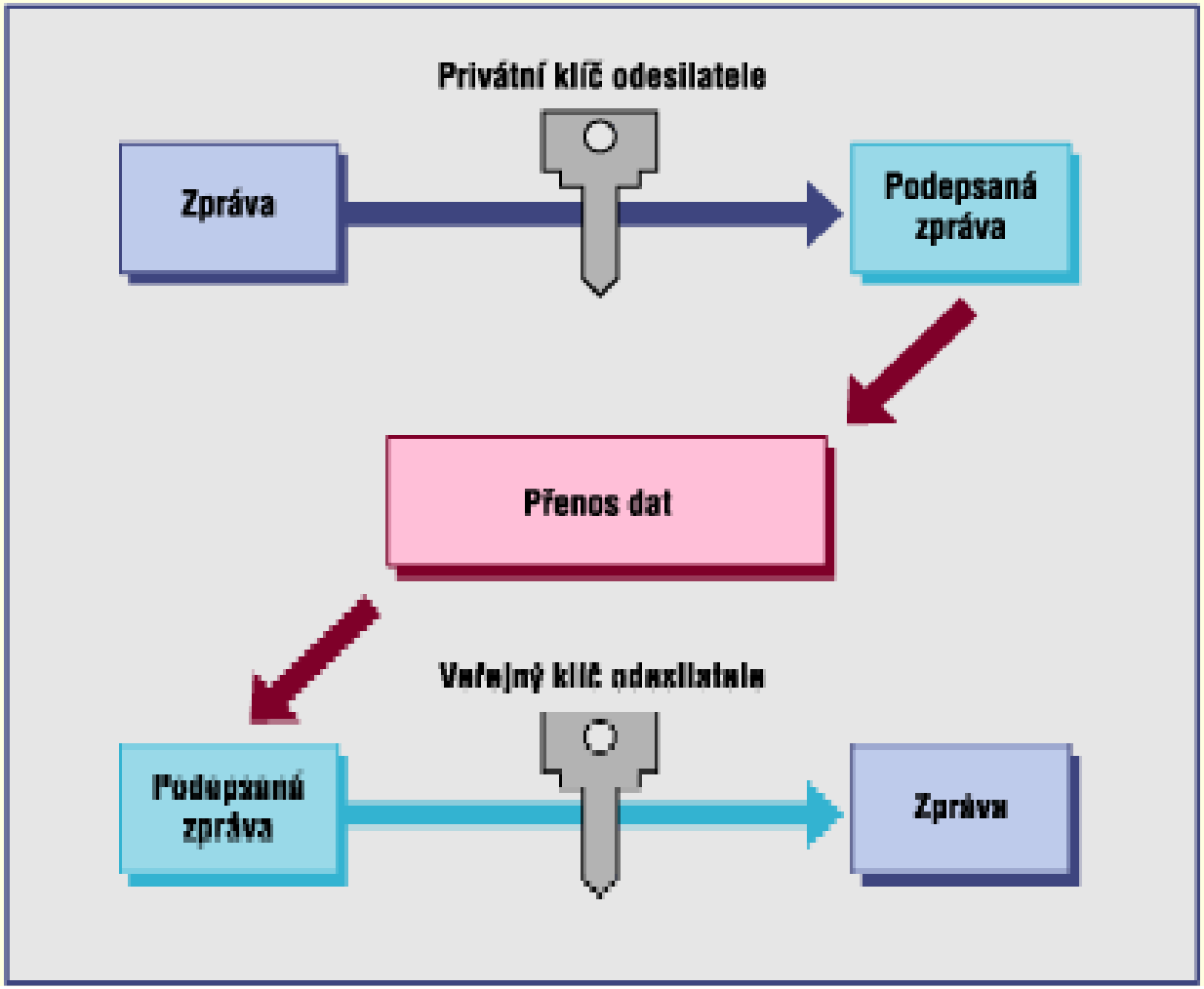
Elektronický podpis

Mezi nejznámější standardy pro asymetrické šifrování patří:

- RSA (Rivest Shamir Adleman - *jména tvůrců algoritmu*)
- DSS (Digital Signature Standard)
- EC (Eliptic Curve).

Elektronický podpis

Asymetrické šifrování

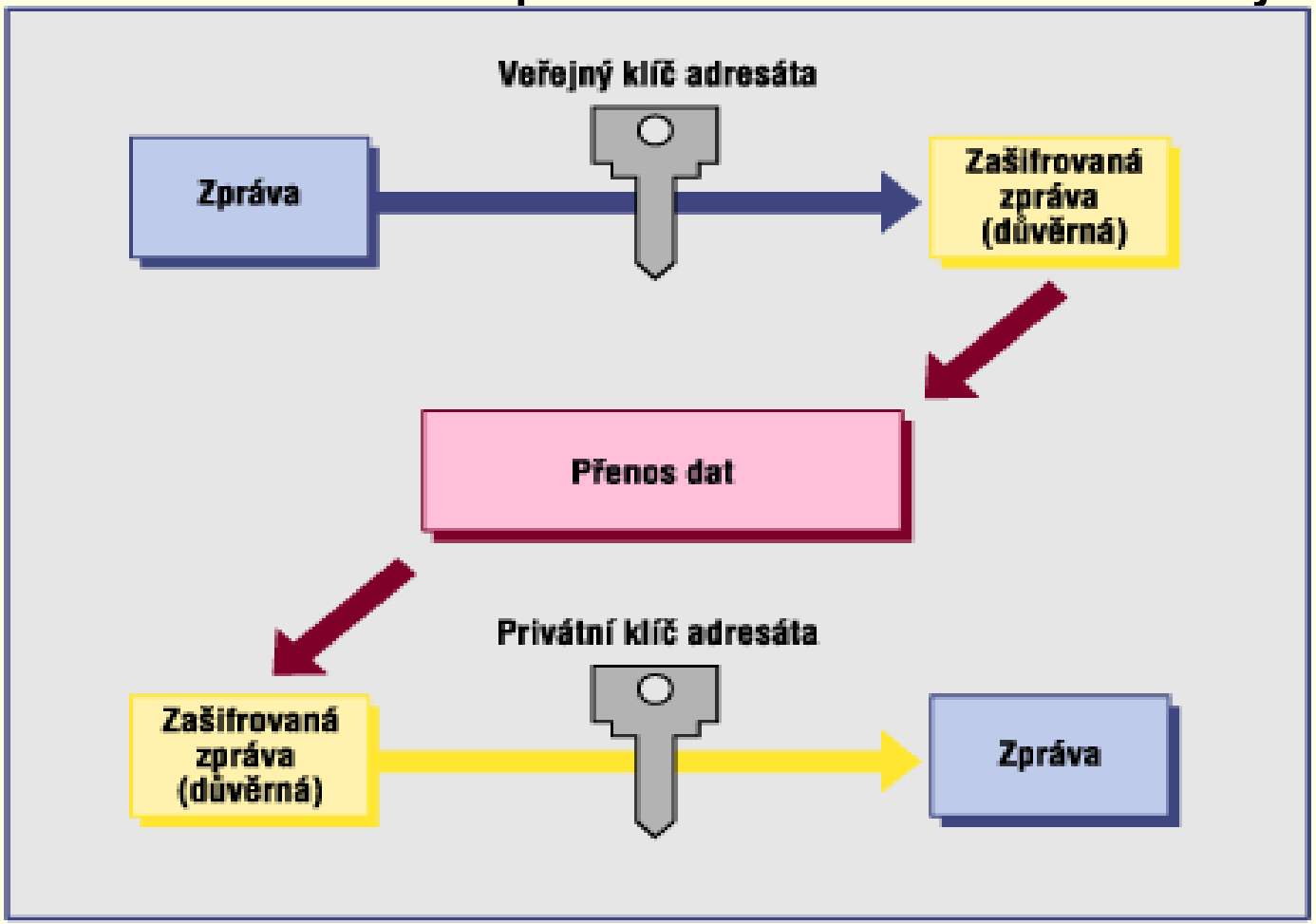


Elektronický podpis

Tímto způsobem lze za pomocí asymetrické kryptografie řešit integritu dat a neodmítnutelnost odpovědnosti na straně odesilatele. Jestliže příjemce pošle podepsané potvrzení o přijetí zprávy, je zajištěna neodmítnutelnost odpovědnosti i ze strany příjemce. Není tak ovšem vyřešena otázka důvěryhodnosti zpráv, tedy nečitelnosti pro neautorizované subjekty. K tomu lze využít šifrování zpráv pomocí veřejného klíče adresáta. Při zašifrování zprávy tímto klíčem máme jistotu, že ji přečte pouze adresát se svým privátním klíčem.

Elektronický podpis

Zajištění nečitelnosti pro neautorizované subjekty

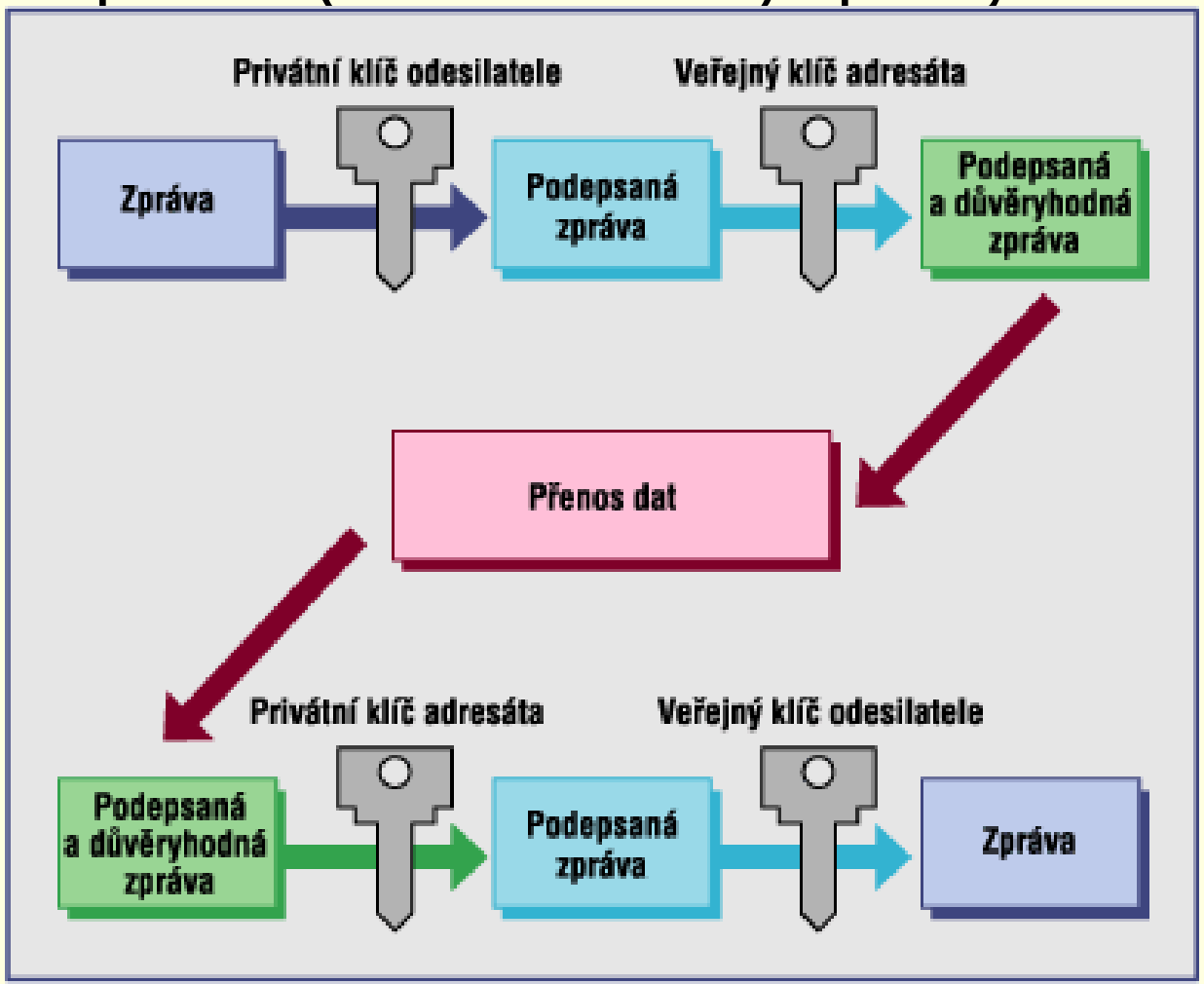


Elektronický podpis

Celý systém pro šifrování a podepisování zpráv pomocí asymetrické kryptografie pracuje tedy následujícím způsobem. Zpráva je obvykle na straně odesilatele nejprve podepsána, podepsán je čitelný text zprávy, a potom šifrována. Na straně příjemce je zpráva nejprve dešifrována privátním klíčem příjemce, čímž je zajištěna adresnost zprávy a teprve potom je pomocí veřejného klíče ověřena identifikace odesilatele.

Elektronický podpis

Přenos adresované, zašifrované (důvěrné) a podepsané (autorizované) zprávy



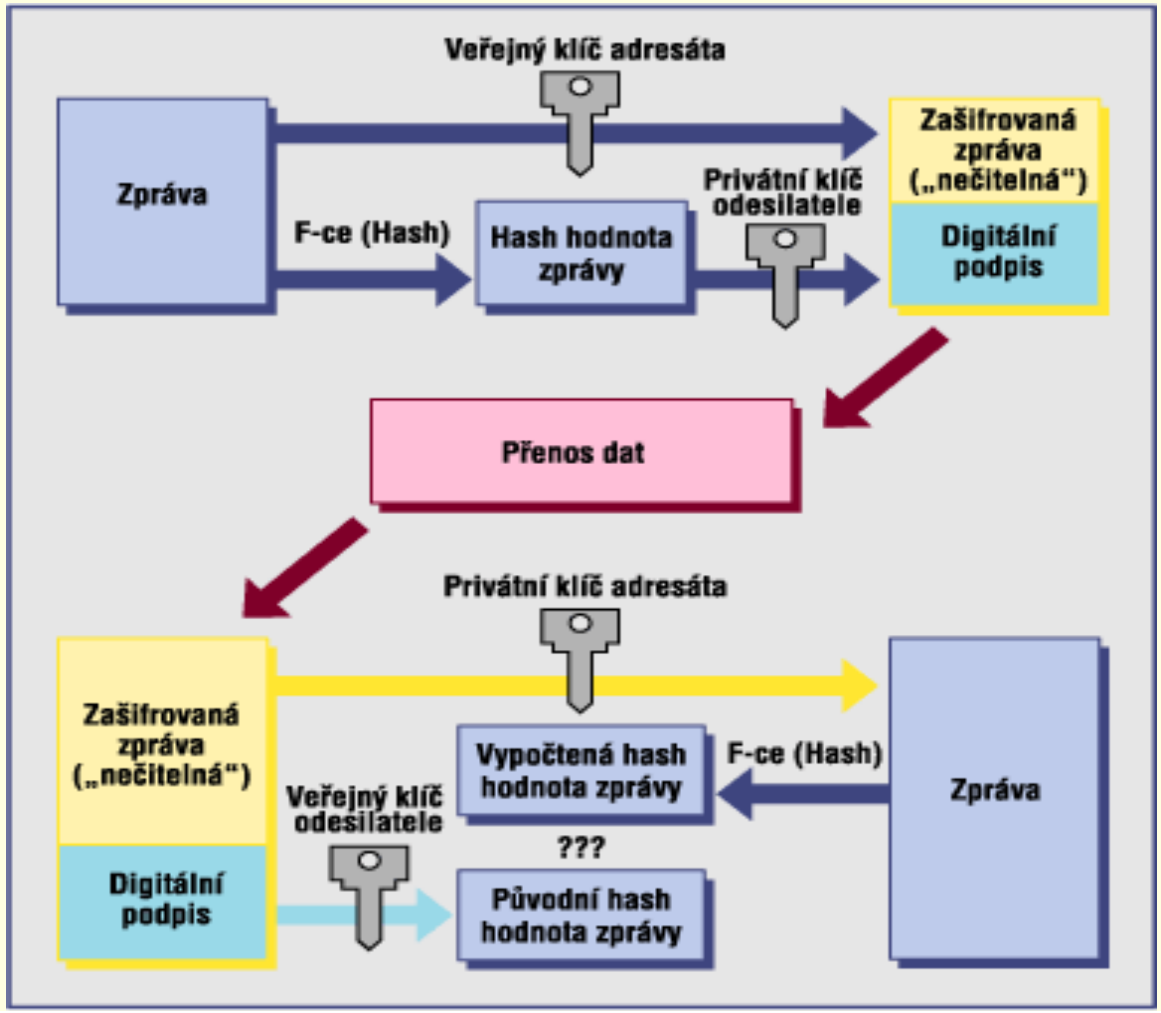
Elektronický podpis

Praktické využití

Aplikace asymetrických algoritmů je výrazně pomalejší než užití algoritmů symetrických. Je to dáno matematickou podstatou asymetrických algoritmů. Proto se mnohdy při tvorbě podpisu nešifruje privátním klíčem odesilatele celá zpráva, ale nejprve se na data použije takzvaná hashovací funkce. Hashovací funkce je jednosměrná transformace, která z variabilních vstupních veličin vrací jednoznačnou hodnotu (textový řetězec) pevné délky, která se jmenuje hash hodnota. Hash hodnota představuje zhuštěnou hodnotu dlouhé zprávy ze které byla vypočtená, ve významu digitálního otisku prstu velkého dokumentu. Opačný proces je nemožný. Příkladem nejznámějších algoritmů hashovacích funkcí jsou MD2 a MD5. Výpočet hash hodnoty zprávy je velmi rychlý. Nejprve se při podpisu zprávy vypočte hash hodnota zprávy, která bývá výrazně kratší než podepisovaná zpráva, a ta se zašifruje některým asymetrickým algoritmem (RSA) s použitím privátního klíče. Výsledkem je takzvaný digitální podpis, který je potom odeslán jako příloha zprávy

Elektronický podpis

- Bezpečná komunikace s využitím digitálního podpisu



Elektronický podpis

Pojmy digitální a elektronický podpis

- Obecnějším pojmem než digitální podpis je pojem ***elektronického podpisu***. Tento pojem v sobě zahrnuje (kromě samotného digitálního podpisu) také aspekty využití celé škály různých biometrických metod. Je pak obvykle precizován tak, aby byl tzv. technologicky nezávislý. Je proto také vhodný pro použití v různých legislativních dokumentech. Zejména v průběhu posledních let se (z hlediska právních a technologických aspektů) dospělo k poznání nezbytnosti používat takto obecný pojem.

Elektronický podpis

Biometrické metody

- *fyziologicky* založené techniky, které měří nějakou fyziologickou charakteristiku dané osoby. Sem patří
- např.: otisky prstů, charakteristiky duhovky, obličej, geometrie cév, charakteristiky uší, vůně, analýza
- obrazců DNA, charakteristiky potu atd.;
- *behaviorálně* založené techniky, které se zabývají měřením chování příslušné osoby. Toto zahrnuje např.: verifikaci ručně psaných podpisů – dynamika podpisu, charakterizace úderů do klávesnice, analýza řečového projevu atd.

Elektronický podpis

V ČR platí:

- zákon č. 227/2000 Sb.,o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), jak vyplývá ze změn provedených zákonem č. 226/2002 Sb., zákonem č. 517/2002 Sb. a zákonem č. 440/2004 Sb.
- http://www.micr.cz/scripts/detail.php?id=1540
- http://www.micr.cz/files/1540/UZ-227_2000.pdf

Elektronický podpis

- **Akreditace pro výkon činnosti akreditovaného poskytovatele certifikačních služeb**
- **1.** První certifikační autorita, a. s.,
  identifikační číslo 26 43 93 95,
  Podvinný mlýn 2178/6, PSČ 190 00 Praha 9
- **2.** Česká pošta, s. p.
  identifikační číslo 47 11 49 83,
  Olšanská 38/9, PSČ 225 99 Praha 3
- **3.** eIdentity a. s.,
  identifikační číslo 27 11 24 89,
  Vinohradská 184/2396, PSČ 130 00 Praha 3

Elektronický podpis

- Zaručený elektronický podpis
- ***Elektronický podpis*** - jsou jím míněna data v elektronickém tvaru, která jsou připojena či logicky asociována k jiným elektronickým datům a která slouží jako metoda autentizace.
- ***Zaručený elektronický podpis***- tím je míněn elektronický podpis splňující následující požadavky:
- (a) je jednoznačně vázán na podepisující osobu;
- (b) umožňuje identifikaci podepisující osoby;
- (c) je vytvořen prostředky, které podepisující osoba může mít pod svojí výhradní kontrolou;
- (d) je vztažen k odpovídajícím datům takovým způsobem, že libovolná následná změna těchto dat je detekovatelná.

Elektronický podpis

- Kvalifikovaný elektronický podpis
- Je to elektronický podpis, který je za prvé zaručený, za druhé založen na kvalifikovaném certifikátu a za třetí byl vytvořen pomocí prostředku pro tzv. bezpečné vytváření podpisů. Poslední pojem „bezpečného“ prostředku je rovněž termínem Direktivy a svým způsobem označuje prostředek, který prošel „validací“, tj. bylo prokázáno, že jeho technologická konstrukce byla provedena tak, aby prostředek splnil celou řadu obsahových i bezpečnostních norem.

Elektronický podpis

- Certifikát a kvalifikovaný certifikát
- ***Certifikát*** **-** elektronické ověření, které propojuje data pro ověření podpisu s osobou a potvrzuje identitu této osoby.
- ***Kvalifikovaný certifikát*** **-** certifikát, který splňuje podmínky uvedené v příloze I a je vydán poskytovatelem certifikačních služeb splňujícím podmínky uvedené v příloze II.
- Příloha I přitom specifikuje, co vše musí kvalifikovaný certifikát obsahovat (identifikace poskytovatele certifikačních služeb, jméno či pseudonym podepsané osoby, pro jaké účely byl certifikát vydán, data pro ověření podpisu, počátek a konec doby platnosti certifikátu, zaručený elektronický podpis příslušného poskytovatele certifikačních služeb, omezení účinnosti certifikátu, atd).

Elektronický podpis

Doplňky zákona

- Jedná se především o tzv. časové razítko, tedy otisk času, který je ke spojen s konkrétními daty. Díky tomu je možné určit, zda konkrétní zpráva existovala v určitém čase.
- Druhou zásadní novinkou je elektronická značka a kvalifikovaný systémový certifikát. Zatímco elektronický podpis je spojen s konkrétní fyzickou osobou, elektronická značka může být generována automaticky, bez zásahu člověka. Například u výpisu z katastru či jiného dokumentu by takto mohlo dojít k automatickému orazítkování pravosti dokumentu.