27. Elektronický podpis (Popis, použité funkce, získání, použití, omezení), certifikáty, zabezpečení dat před zneužitím a před ztrátou. Definujte a uveďte příklady využití redundance dat.

Elektronický podpis

Popis

- Elektronický podpis (též digitální podpis) je v informatice označení specifických dat, které v počítači nahrazují klasický vlastnoruční podpis, respektive ověřený podpis.
- Je připojen k datové zprávě nebo je s ní logicky spojen, takže umožňuje ověření totožnosti podepsané osoby ve vztahu k datové zprávě.
- Elektronický podpis je prostředek k tomu, jak v anonymním světě internetu ověřit totožnost odesílatele.
- Z právního hlediska je elektronický podpis definován jako data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání.
- Elektronický podpis je vytvořen pro konkrétní data a je možné pomocí počítače ověřit, zda je platný a zda jsou data v té podobě, ve které byla podepsána.
- Součástí elektronického podpisu je identifikace toho, kdo podpis vytvořil.
- Ověření elektronického podpisu zahrnuje kromě matematických operací i přenos důvěry z důvěryhodné třetí strany na tvůrce podpisu a následně na důvěryhodnost elektronicky podepsaného dokumentu.
- Pro ověření důvěryhodnosti se využívá digitální certifikát, vydaný certifikační autoritou.

Vlastnosti elektronického podpisu

Autenticita

- Lze ověřit identitu subjektu, kterému patří elektronický podpis.
- Autenticita je realizována pomocí přenosu důvěry.

Integrita

- Lze prokázat, že od vytvoření elektronického podpisu nedošlo k žádné změně v podepsaném dokumentu, tj. že dokument (podepsaný soubor) není úmyslně či neúmyslně poškozen.

Nepopiratelnost

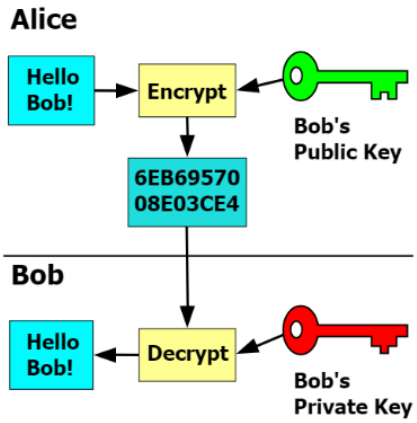
- Autor nemůže tvrdit, že elektronický podpis příslušný k dokumentu nevytvořil.
- Důvodem je fakt, že pro vytvoření elektronického podpisu je potřeba privátní klíč, který je těsně svázán s veřejným klíčem, pomocí kterého dochází k matematickému ověření elektronického podpisu.
- Bez přístupu k privátnímu klíči nelze elektronický podpis vytvořit a ověření elektronického podpisu může být provedeno jen veřejným klíčem, který k němu patří.

Časové ukotvení

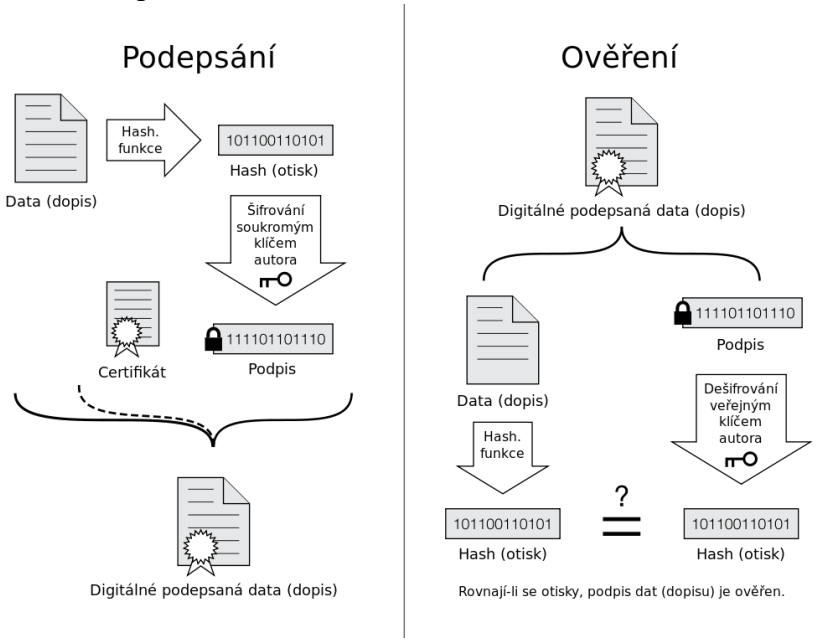
- Elektronický podpis může obsahovat časové razítko, které prokazuje datum a čas podepsání dokumentu.

- Časové razítko vydává důvěryhodná třetí strana, a protože je součástí elektronického podpisu, lze ji ověřit stejným postupem, jako elektronický podepsaný dokument.

Použité funkce



- Princip elektronického podpisu vychází z existence nějaké soukromé informace, kterou vlastní jenom podepisující osoba a nikdo jiný, a tato informace reprezentuje jeho schopnost vytvořit elektronický podpis pod určitým dokumentem.
- Toto číslo je tajnou informací – daty pro vytvoření elektronického podpisu.
- U elektronického podpisu podepisování probíhá velmi podobně jako na papíru, přičemž místo papírového dokumentu je k dispozici elektronický dokument (v podstatě jedno velmi velké číslo) a místo podpisové schopnosti existuje druhé číslo – tajné podepisovací číslo.
- Určitým matematickým spojením těchto dvou čísel vzniká číslo nové, a tím je právě elektronický podpis.
- Ten je možné připojit k podepisovanému dokumentu, přenášet jej s ním na dálku – např. e-mailem, uložit podepsaný dokument na jakékoliv médium umožňující digitální záznam apod.



- Podepsání elektronického dokumentu probíhá tak, že se „prožene“ speciálním programem, který vygeneruje z obsahu dokumentu a ze soukromého klíče určitou posloupnost znaků, kterou připojí ke zprávě jako její digitální podpis.
- Takto podepsaná zpráva je odeslána příjemci.
- Příjemce použije druhý klíč, komplementární k předchozímu – tzv. veřejný klíč, pomocí nějž může ověřit pravost podpisu (tj. provést identifikaci a autentizaci odesilatele) a neporušenost obsahu (integritu) zprávy.

Získání

1. Rozmyslím si, v jakém právním vztahu budu se svým certifikátem vystupovat.
2. Připravím si smlouvu a dokumentaci ve dvojím vyhotovení.
3. Pokud chci kvalifikovaný elektronický podpis, objednám si kvalifikovaný prostředek na www.postshop.cz
4. Vygeneruji si žádost o certifikát pomocí aplikace iSignum.
5. S dokumenty, vygenerovaným číslem žádosti (ID žádosti) a dokladem totožnosti pro vydání certifikátu se vydám na pobočku ČP se službou Czech POINT nebo my přijedeme za Vámi!
6. Na zadaný e-mail Vám po návštěvě pobočky dorazí informace o vydání certifikátu. Nainstalujte ho dle zaslaných pokynů. Případně nahlédněte do sekce Návodů
7. Hotovo

Použití

- Při podání přehledu o příjmech a výdajích OSVČ
- Při elektronické komunikaci se státní správou
- Při elektronické komunikaci s krajskými a městskými úřady
- Při elektronické komunikaci se zdravotními pojišťovnami
- Při žádosti o sociální dávky
- Při podávání žádostí o dotace EU
- Při použití datové schránky
- Při podepisování faktur
- Jako elektronický podpis PDF dokumentů

Omezení

- Nevýhodou certifikátů je jejich omezená platnost. Prošlý certifikát by totiž zapříčinil neplatnost podpisu, a je proto nezbytné, aby byla platnost certifikátu každý rok prodloužena.
- Veřejné CA postrádají akreditaci, která je potřeba např. pro komunikaci se státní správou. Akreditované certifikáty mohou vydat pouze akreditované subjekty.

Úrovně elektronických podpisů

Zaručený elektronický podpis

- Jedná se o elektronický podpis, který je vytvořen na základě soukromého klíče a k němu náležícímu certifikátu.
- Použitý certifikát nemusí splňovat žádné speciální náležitosti a může tedy být vydán jakoukoli certifikační autoritou, nebo může být tzv. self-signed.

Uznávaný elektronický podpis

- Jedná se o zaručený elektronický podpis, k jeho vytvoření byl navíc použit tzv. kvalifikovaný certifikát.
- Takový certifikát vydávají za úplatu kvalifikované certifikační autority.

Kvalifikovaný elektronický podpis

- Jedná se o nejvyšší úroveň elektronického podpisu.
- Základem je opět zaručený podpis a pro vytvoření této úrovně elektronického podpisu musí podepisující disponovat kvalifikovaným certifikátem a dále musí disponovat kvalifikovaným prostředkem pro vytváření elektronických podpisů, na kterém je uložen soukromý klíč podepisujícího.

Jiné typy elektronických podpisů

- Jedná se o takové elektronické podpisy, které nejsou vytvořeny dle principů asymetrické kryptografie, ale ze své podstaty jsou stále elektronické. V praxi se jedná např. o:
    - Biometrické podpisy,
    - Jméno a příjmení v patičce emailu,
    - Naskenovaný obrázek vlastnoručního podpisu apod.

Certifikáty

- Podle zákona certifikát vystavuje poskytovatel certifikačních služeb, což je soukromoprávní subjekt, poskytující službu spočívající v propojení fyzické osoby s jejím veřejným klíčem prostřednictvím tzv. certifikátu.
- Certifikátem zaručuje, že veřejný klíč patří opravdu tomu, kdo je označen jako jeho vlastník.
- Certifikát je tedy také elektronický dokument, který k tomu, aby mohl sloužit svému účelu, musí být elektronicky podepsán poskytovatelem certifikačních služeb. (Tím je chráněn jeho obsah proti zásahu podobně, jako jiné podepsané elektronické dokumenty.)
- Může dokonce existovat více certifikátů, má-li osoba více dvojic klíčů, určených pro různé příležitosti. Jeden jako soukromá osoba, jeden jako statutární představitel firmy, jeden jako člen zájmového spolku apod.
- Certifikát může obsahovat i pověření osoby nebo limit transakcí, které lze takto podepsat.

Poskytovatelé certifikačních služeb

Akreditované certifikační autority

- Tyto certifikáty, které mohou pochopitelně vydat pouze akreditované subjekty, mají nejširší možnost použití.
- Samostatný proces akreditace nám zaručuje velice dobrou jistotu zejména o bezpečnosti takových certifikátů a o tom, poskytovatel disponuje dostatečnými prostředky na krytí případných škod.

Veřejné CA

- Do další skupiny spadají certifikační autority, které sice nemají akreditaci, ale nabízejí své certifikační služby veřejnosti.

Soukromé CA

- Typické je, že tyto autority nevydávají certifikáty široké veřejnosti.
- Certifikáty jsou vydávány pro potřeby organizace, nebo jejich partnerů klientů apod.

Zabezpečení dat před zneužitím a před ztrátou

Zabezpečení dat před zneužitím

- Zničení (skartace, spalování)
- Autorizovaný přístup – Bezpečnostní politika firmy
- Hesla
- Biometrie
- Nároky na ochranu dat rostou s množstvím uživatelů a interaktivitou jejich práce.

Zabezpečení dat před ztrátou

- Zálohování

- Distribuovaná báze dat X Centralizovaná báze dat
- Cloudy

Definujte a uveďte příklady využití redundance dat

- Redundance uvádí míru nadbytečnosti.

$$r = 1 - h = \frac{H_{max} - H}{H_{max}} \cdot 100\ \%$$

- Způsobuje, že musíme přenášet více symbolů než v optimálním kódu.
- Redundance je často plánovaná, např. Zabezpečující kódy.
- Maximální redundance – opakování celé zprávy → 100%

Hammingova vzdálenost

- Udává počet míst, ve kterých se budou dvě sousední slova vzájemně lišit.
- Hammingova vzdálenost je nejmenší počet pozic, na kterých se řetězce stejné délky daného kódu liší neboli počet záměn, které je potřeba provést pro změnu jednoho z řetězců na druhý.
- $\rho = 1$ bez redundance
- $\rho = 2$ lze detekovat chybu
- $\rho \geq 3$ lze chybu opravit

Přenosový kanál

$$C = B \log_2 \left(1 + \frac{S}{N}\right) [bps]$$

- C – kapacita
- B - šířka