Variace

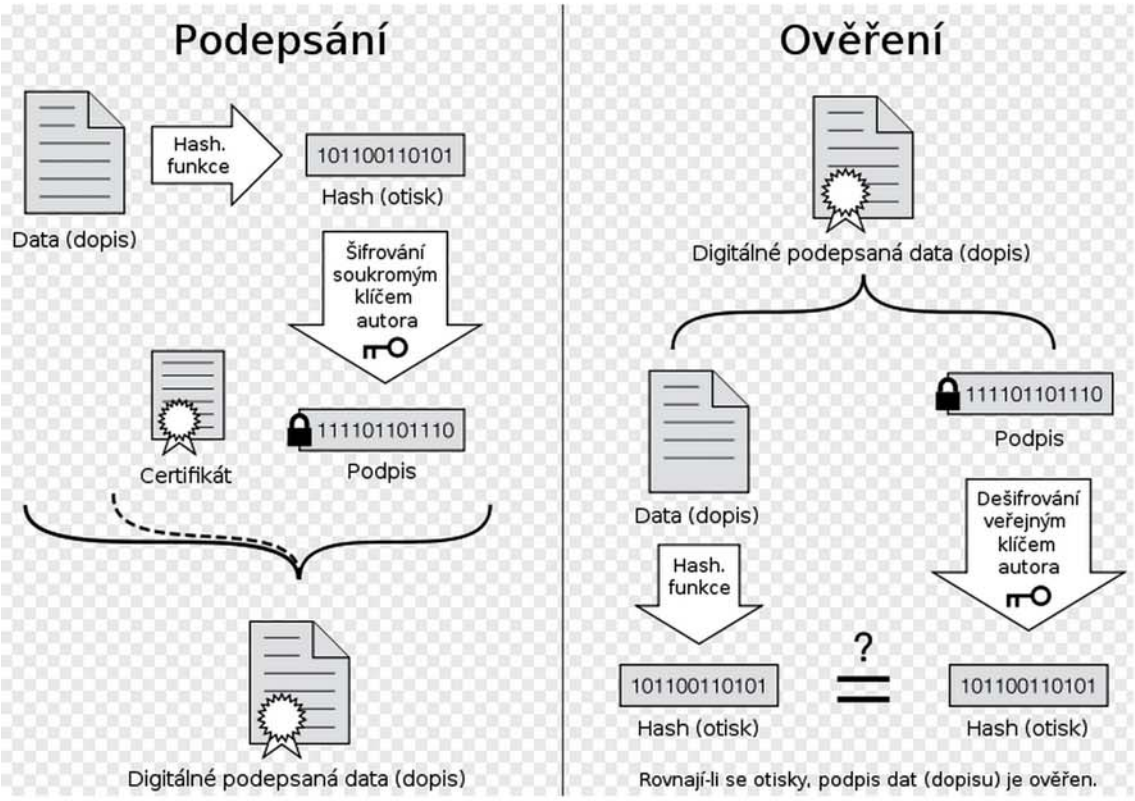
1

Elektronický podpis

Autor: Mgr. Jaromír JUŘEK

1. Elektronický podpis

Elektronický podpis (též digitální podpis) je v informatice označení specifických dat, které v počítači nahrazují klasický vlastnoruční podpis. Svou věrohodností se považuje za **důvěryhodnější než je notářsky ověřený podpis**. Elektronický podpis je vytvořen pro konkrétní data a je možné pomocí počítače ověřit, zda je platný (obdoba písmoznalectví). 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. K tomu se využívá digitální certifikát a certifikační autorita nebo síť důvěry.



Vlastnosti elektronického podpisu:

- **Autenticita** - znamená, že lze ověřit identitu subjektu, kterému patří elektronický podpis. Autenticita je realizována pomocí přenosu důvěry.
- **Integrita** - pomocí integrity 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** - znamená, že 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.

Elektronický podpis vydává společnost, které se říká certifikační autorita. V naší republice se v současné době zúžila nabídka certifikačních autorit do dvou hlavních. První z nich je První certifikační autorita (ICA), jejíž internetové stránky jsou www.ica.cz a dále certifikační autorita Postsignum, kterou provozuje Česká pošta ve své síti Czechpoint. Internetová adresa této autority je www.postsignum.cz.

Obvyklý postup při požadavku na zřízení elektronického podpisu:

1. Nainstalovat si do počítače veřejný klíč certifikační autority, kterou jsme se rozhodli využít (v některých operačních systémech se staženými všemi aktualizacemi už může být implementován).

2. Vygenerovat elektronickou žádost přes webový prohlížeč a následně ji uložit na přenosné médium (např. USB flash disk); vytisknout formulář žádosti a ten zatím nepodepisovat.

3. Zajít na nejbližší pobočku Czechpointu, případně pracoviště ICA, tam předložit data na přenosném médiu a po prokázání totožnosti (např. občanským průkazem) před zraky obsluhujícího personálu formulář podepsat. Pokud je toto pracoviště méně dostupné (např. v menších obcích), lze žádost odeslat i doporučeným dopisem na adresu uvedenou na internetových stránkách. V tom případě, ale musí být podpis úředně ověřen.

4. Zaplatit společností stanovený poplatek (obvykle cca 400 Kč s platností podpisu na jeden rok).

5. Po zavedení všech potřebných dat do systému, nahraje elektronický podpis pracovník certifikační autority na dodané přenosné médium, případně v poslední době častěji tento soubor odešle na e-mailovou adresu, k níž je certifikát vystaven.

POZOR! Certifikát, který je připojen jako příloha e-mailu lze zpravidla nainstalovat pouze jednou! Tedy při chybě nebo zhavarování postupu je nutno znovu podat žádost a vše opakovat.

POZOR! Od doby podání žádosti až do doby doinstalování certifikátu nesmí být v počítači reinstalován operační systém, ani v něm nesmí být prováděny žádné větší aktualizace.

Po úspěšném nainstalování certifikátu lze privátní klíč, uložený v počítači při podání žádosti odstranit, a úspěšně nainstalovaný certifikát následně vyexportovat a uložit na bezpečné místo.

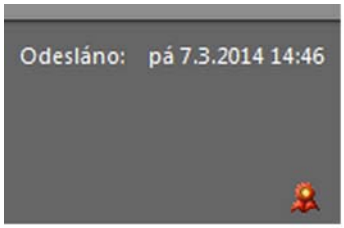
V české legislativě je definován **zaručený elektronický podpis**, který vyhovuje uznávání státní správou (zákon č. 227/2000 Sb., o elektronickém podpisu). Zákon byl několikrát novelizován a odpovídá evropské legislativě a obdobným zákonům v ostatních státech světa. Zákon rozlišuje elektronický podpis, který identifikuje fyzickou osobu a právnickou osobu, která se prokazuje elektronickou značkou (obdoba firemního nebo úředního razítka).

Využití zaručeného podpisu

- při podání přehledu o příjmech a výdajích OSVČ
- u přihlášky a odhlášky k nemocenskému pojištění
- u přiznání k DPH
- 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

Ukázka doručeného e-mailu s ověřenou platností elektronického podpisu:

Detail ikony ověření:



Ukázka doručeného e-mailu, kde není ověřena pravost elektronického podpisu (detail ikony):

Pokud majitel elektronického podpisu nedokázal z jakýchkoliv důvodů ochránit soubor certifikátu (např. při krádeži počítače, ztrátě přenosného média, apod.), může certifikační autoritu **požádat o předčasné zneplatnění certifikátu** ještě před datem, kdy měla jeho platnost oficiálně skončit.

Obsah