Elektronický podpis

Elektronický podpis

- Elektronický podpis x vlastnoruční podpis
- Dva stupně elektronického podpisu:
  - obyčejný
  - zaručeny

Digitální podpis

- Je „číslo“
- Využívá se šifrovacích algoritmů:
  - symetrických
  - asymetrických
- Je spojení digitálního dokumentu s privátním klíčem
- Ověření pravosti – pomocí veřejného klíče
- Zaručení pravosti pomocí certifikátů

Zákon 227/2000 Sb. o elektronickém podpisu

- Pro účely tohoto zákona se rozumí **elektronickým podpisem** 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

Zaručený elektronický podpis

- Je elektronický podpis, který splňuje následující požadavky:
  - je jednoznačně spojen s podepisující osobou,
  - umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
  - byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
  - je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

Elektronická značka

- Jsou údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky:
  - jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu,
  - byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou,
  - jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat.

Definiční pojmy

- *datovou zprávou elektronická data*, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou,
- *podepisující osobou fyzická osoba*, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby,
- *označující osobou fyzická osoba*, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou,
- *držitelem certifikátu fyzická osoba*, právnická osoba nebo organizační složka státu, která požádala o vydání kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu pro sebe nebo pro podepisující nebo označující osobu a které byl certifikát vydán,
- *poskytovatelem certifikačních služeb fyzická osoba*, právnická osoba nebo organizační složka státu, která vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy,
- *kvalifikovaným poskytovatelem certifikačních služeb* poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty nebo kvalifikovaná časová razítka nebo prostředky pro bezpečné vytváření elektronických podpisů (dále jen „kvalifikované certifikační služby") a splnil ohlašovací povinnost podle § 6,
- *akreditovaným poskytovatelem certifikačních služeb* poskytovatel certifikačních služeb, jemuž byla udělena akreditace podle tohoto zákona,

- *certifikátem datová zpráva*, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu,
- *kvalifikovaným certifikátem certifikát*, který má náležitosti podle zákona a byl vydán kvalifikovaným poskytovatelem certifikačních služeb,
- *kvalifikovaným systémovým certifikátem certifikát*, který má náležitosti podle zákona a byl vydán kvalifikovaným poskytovatelem certifikačních služeb
- daty pro vytváření elektronických podpisů jedinečná data, která podepisující osoba používá k vytváření elektronického podpisu,
- daty pro ověřování elektronických podpisů jedinečná data, která se používají pro ověření elektronického podpisu,
- daty pro vytváření elektronických značek jedinečná data, která označující osoba používá k vytváření elektronických značek,
- daty pro ověřování elektronických značek jedinečná data, která se používají pro ověření elektronických značek,
- *kvalifikovaným časovým razítkem datová zpráva*, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem,
- prostředkem pro vytváření elektronických podpisů technické zařízení nebo programové vybavení, které se používá k vytváření elektronických podpisů,

- *prostředkem pro ověřování elektronických podpisů* technické zařízení nebo programové vybavení, které se používá k ověřování elektronických podpisů,
- prostředkem pro bezpečné vytváření elektronických podpisů prostředek pro vytváření elektronického podpisu, který splňuje požadavky stanovené tímto zákonem,
- prostředkem pro bezpečné ověřování elektronických podpisů prostředek pro ověřování podpisu, který splňuje požadavky stanovené tímto zákonem,
- *nástrojem elektronického podpisu* technické zařízení nebo programové vybavení, nebo jejich součásti, používané pro zajištění certifikačních služeb nebo pro vytváření nebo ověřování elektronických podpisů,
- *prostředkem pro vytváření elektronických značek zařízení*, které používá označující osoba pro vytváření elektronických značek a které splňuje další náležitosti stanovené tímto zákonem,
- elektronickou podatelnou pracoviště orgánu veřejné moci určené pro příjem a odesílání datových zpráv,
- akreditací osvědčení, že poskytovatel certifikačních služeb splňuje podmínky stanovené tímto zákonem pro výkon činnosti akreditovaného poskytovatele certifikačních služeb.

Soulad s požadavky na podpis

- Datová zpráva je podepsána, pokud je opatřena elektronickým podpisem. Pokud se neprokáže opak, má se za to, že se podepisující osoba před podepsáním datové zprávy s jejím obsahem seznámila.
- Použití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu umožňuje ověřit, že datovou zprávu podepsala osoba uvedená na tomto kvalifikovaném certifikátu.

Soulad s originálem

- Použití zaručeného elektronického podpisu nebo elektronické značky zaručuje, že dojde-li k porušení obsahu datové zprávy od okamžiku, kdy byla podepsána nebo označena, toto porušení bude možno zjistit.

Další ustanovení zákona

- Povinnost podepisující a označující osoby § 5
- Povinnosti poskytovatele certifik. služeb §6
- Akreditace a dozor

Náležitosti kvalifikovaného certifikátu

(1) Kvalifikovaný certifikát musí obsahovat

a) označení, že je vydán jako kvalifikovaný certifikát podle tohoto zákona,

b) obchodní jméno poskytovatele certifikačních služeb a jeho sídlo, jakož i údaj, že certifikát byl vydán v České republice,

c) jméno a příjmení podepisující osoby, nebo její pseudonym s příslušným označením, že se jedná o pseudonym,

d) zvláštní znaky osoby, vyžaduje-li to účel kvalifikovaného certifikátu,

e) data pro ověření podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby,

f) zaručený elektronický podpis poskytovatele certifikačních služeb, který kvalifikovaný certifikát vydává,

g) číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb,

h) počátek a konec platnosti kvalifikovaného certifikátu,

i) případně údaje o tom, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití,

j) případně omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít.

(2) Další osobní údaje smí kvalifikovaný certifikát obsahovat jen se svolením podepisující osoby.