

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Není elektronický podpis jako elektronický podpis

Při své činnosti podnikatelé čím dál častěji jednají tzv. online za použití elektronického podpisu, ať již jde o vystupování vůči domovským úřadům a institucím (finanční úřady, soudy, správa sociálního zabezpečení, celní správa), případně úřadům a institucím jiného státu, nebo o jednání s obchodními partnery, českými i zahraničními. Přitom se mohou setkat s několika typy elektronických podpisů, kdy nemusí být na první pohled zřejmé, který z nich má být použit a zda jeho použití přinese jednáním výhody, pro něž k jeho použití přistoupili.

V podmínkách českého právního prostředí se můžeme v rámci elektronického podepisování soukromoprávními subjekty setkat s těmito typy elektronických podpisů:

1. prostý elektronický podpis ve smyslu čl. 3 bod 10) nařízení eIDAS[1], resp. ve smyslu ustanovení § 7 zákona o službách vytvářejících důvěru pro elektronické transakce (dále jen „ZSVDET“)[2];
2. zaručený elektronický podpis ve smyslu čl. 26 eIDAS, resp. zaručený elektronický podpis ve smyslu ustanovení § 6 odst. 2 ZSVDET;
3. kvalifikovaný elektronický podpis ve smyslu ustanovení čl. 3 eIDAS, resp. kvalifikovaný elektronický podpis a ustanovení § 6 odst. 2 ZSVDET.

Prostý elektronický podpis

Jedná se o nástroj, který je představován daty v elektronické podobě připojenými k jiným datům v elektronické podobě nebo s nimi logicky spojenými, která podepisující osoba používá k podepsání. Může mít formu napsání jména v e-mailu či v elektronickém dokumentu, naskenovaného vlastnoručního podpisu, e-mailové patičky či vzorku vlastnoručního podpisu vytvořeného na nějakém dotykovém zařízení. Prostý elektronický podpis je taktéž možno vytvořit v různých platformách (např. DocuSign) či aplikacích (např. Adobe Acrobat), jejichž prostřednictvím může být podepisování dokumentů realizováno (podepisujícímu je nabídnut již vytvořený podpis, který si může dle vlastních představ upravit).

Tento podpis má své využití při jednání mezi soukromoprávními subjekty, pokud není stranami sjednáno či zákonem vyžadováno jinak. Nevypovídá však nic o totožnosti podepisujících ani o nezměněnosti obsahu podepisovaného dokumentu, a nelze jej použít při jednání s českým veřejnoprávním podepisujícím[3], resp. při využití určité on-line služby, která je poskytována subjektem veřejného sektoru[4] nebo jeho jménem.

Zaručený elektronický podpis

Zaručený elektronický podpis je elektronický podpis založený na kvalifikovaném certifikátu vydaném kvalifikovaným poskytovatelem služeb vytvářejících důvěru (dále jen „**kvalifikovaný poskytovatel**“). Tento podpis musí být jednoznačně spojen s podepisující osobou, umožňovat identifikaci podepisující osoby, být vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou, a být k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv

následnou změnu dat[5].

Aktuální seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru v ČR je dostupný na oficiálních stránkách Evropské unie [zde](#), nejčastěji se přitom setkáváme s certifikáty vydanými společnostmi První certifikační autorita, a.s. (I.CA), Certifikační autorita PostSignum – Česká pošta či eIdentity a.s. Aktuální seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru v EU je dostupný na oficiálních stránkách Evropské unie [zde](#).

Pro zřízení zaručeného elektronického podpisu je s kvalifikovaným poskytovatelem na základě předem vygenerované žádosti uzavřena smlouva o poskytování certifikačních služeb a ověřena totožnost subjektu, jemuž je kvalifikovaný certifikát zřizován. V případě českých kvalifikovaných poskytovatelů je totožnost konkrétně dokládána dvěma osobními doklady (v případě nepodnikající fyzické osoby) či jedním osobním dokladem (v případě podnikající fyzické osoby). Vydaný kvalifikovaný certifikát a jemu příslušná data (tzv. soukromý klíč[6] a veřejný klíč[7]) mohou být umístěna přímo v počítači či jiném zařízení, na němž je zaručený elektronický podpis vytvářen. Tento podpis lze stejně jako prostý elektronický podpis použít k podpisu e-mailu, či jej přímo vložit do podepisovaného dokumentu.

Zaručený elektronický podpis se použije při podpisu soukromoprávního elektronického dokumentu, bylo-li to stranami sjednáno, a elektronického dokumentu, kterým se činí úkon vůči českému veřejnoprávnímu podepisujícímu nebo jiné osobě v souvislosti s výkonem její působnosti[8], příp. při využití určité on-line služby, která je poskytována subjektem veřejného sektoru nebo jeho jménem[9].

Kvalifikovaný elektronický podpis

Tento typ elektronického podpisu představuje v současnosti nejvyšší úroveň podpisu. Jde o elektronický podpis založený na kvalifikovaném certifikátu pro elektronické podpisy vydaném kvalifikovaným poskytovatelem služeb vytvářejících důvěru (stejně jako v případě zaručeného elektronického podpisu), který je ovšem navíc vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů[10] (dále jen „**kvalifikovaný prostředek**“).

Na kvalifikovaném prostředku jsou uloženy jak soukromý klíč i kvalifikovaný certifikát (s veřejným klíčem)[11]. Soukromý klíč nelze z kvalifikovaného prostředku vyexportovat. Seznam kvalifikovaných prostředků pro vytváření elektronických podpisů zřizovaných kvalifikovanými poskytovateli v jednotlivých státech EU je dostupný na oficiálních stránkách Evropské unie [zde](#). V případě kvalifikovaného certifikátu zřizovaného českými kvalifikovanými poskytovateli může kvalifikovaným prostředkem být certifikovaná čipová karta (např. eObčanka vydaná od 01.07.2018)[12] nebo jiný externí nosič (např. USB token). Bez použití tohoto nosiče není možné dokument řádně elektronicky podepsat.

I v tomto případě je se zřizujícím kvalifikovaným poskytovatelem uzavřena smlouva o poskytování certifikačních služeb a ověřena totožnost žadatele. Žádost o vydání kvalifikovaného certifikátu je ovšem již třeba vygenerovat na kvalifikovaném prostředku, na nějž bude kvalifikovaný certifikát uložen. Kvalifikovaný prostředek je možné objednat přímo u kvalifikovaného poskytovatele, příp. si zakoupit jakýkoliv kvalifikovaný prostředek uvedený na seznamu kvalifikovaných prostředků[13]. I kvalifikovaný elektronický podpis použít k podpisu e-mailu, či jej přímo vložit do podepisovaného dokumentu.

Kvalifikovaný elektronický podpis umožňuje komunikaci se všemi orgány veřejné moci, a to i v rámci přeshraničního styku. Pro úplnost dodejme, že orgány veřejné moci jsou povinny podepisovat elektronické dokumenty jedině kvalifikovaným elektronickým podpisem[14].

Pro zaručený elektronický podpis a kvalifikovaný elektronický podpis zavádí ZSVDET v ustanovení §6 odst. 2 legislativní zkratku uznávaný elektronický podpis. Byť oba podpisy naplňují kritéria bezpečné komunikace mezi občany, zejména co se nezměněného obsahu podepisovaných dokumentů a totožnosti podepisujících subjektů týká, jen druhý z nich je v souladu s nařízením eIDAS uznáván jako kvalifikovaný podpis ve všech členských státech Evropské unie a má také ve všech členských státech Evropské unie právní účinek rovnocenný vlastnoručnímu podpisu[15].

Závěrem

Přestože existuje více druhů elektronických podpisů, které mohou soukromoprávní subjekty používat, v rámci právní jistoty lze doporučit využívat kvalifikovaný elektronický podpis. Jeho použití není pro běžného uživatele nijak obtížné, když certifikát uložený na externím nosiči je běžné využívan např. při přístupu do elektronického bankovníctví, a rovněž instrukce pro připojení podpisu v jednotlivých platformách či aplikacích jsou velmi srozumitelné i tzv. laikům.

Tento druh podpisu představuje v současnosti nejvyšší úroveň podpisu a stupeň zabezpečení, a má tak nejširší rozsah použití v rámci celé Evropské unie (mimo ni pak v souladu s dohodou soukromoprávních subjektů či požadavky cizích orgánů státní moci). Jeho použití lze rovněž doporučit v případě elektronicky uzavíraných smluv, kde bylo stranami dohodnuto, či je zákonem vyžadováno dodržení písemné formy (tedy např. zástavní smlouva, smlouva o převodu nemovitosti, pojistná smlouva uzavřená na dobu alespoň 1 roku apod.).

Současně je však třeba uvést, že při vědomí aktuálního stále sílícího trendu digitalizace a elektronizace (nejen) právních jednání eIDAS stanoví, že *Elektronickému podpisu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy*[16]. Tedy i prostý elektronický podpis je způsobilým prostředkem k uzavření smlouvy, u níž není stranami sjednáno či zákonem vyžadováno jinak.



Mgr. Hana Trusíková
advokát



Doležal & Partners s.r.o., advokátní kancelář

Růžová 1416/17
110 00 Praha

Koliště 1912/13
602 00 Brno

tel.: +420 222 544 201

e-mail: office@dolezalpartners.com

[1] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23.07.2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

[2] Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších změn.

[3] Stát, územní samosprávný celek, právnická osoba zřízená zákonem nebo právnická osoba zřízená nebo založená státem, územním samosprávným celkem nebo právnickou osobou zřízenou zákonem nebo jejich orgán anebo jiná jejich součást, příp. jiná právnická osoba, jedná-li při výkonu své působnosti (srov. §5 SZVDET).

[4] Státní, regionální nebo místní orgán, veřejnoprávní subjekt, sdružení vytvořené jedním nebo několika takovými orgány nebo jedním nebo několika takovými veřejnoprávními subjekty nebo soukromý subjekt, který byl alespoň jedním z těchto orgánů, subjektů nebo sdružení pověřen poskytovat veřejné služby, jedná-li na základě tohoto pověření (srov. čl. 3 bod 7) a bod 8) eIDAS.

[5] Srov. čl. 26 eIDAS.

[6] Soukromý klíč obsahuje data pro tvorbu elektronického podpisu.

[7] Veřejný klíč obsahuje data pro ověření podpisu.

[8] Srov. §6 odst. 1 ZSVDET.

[9] Srov. čl. 27 odst. 2 eIDAS.

[10] QSCD - qualified signature creation device (srov. čl. 3 bod 23) a Přílohu II. eIDAS).

[11] Generování klíče a žádosti kvalifikovaným poskytovatelem se v tomto případě provádí přímo na kvalifikovaný prostředek.

[12] Čip eObčanky musí uživatele aktivovat a pro její použití při vytváření elektronického podpisu je nutné mít k dispozici čtečku čipových karet.

[13] Dostupný na oficiálních stránkách Evropské unie [zde](#).

[14] Srov. §5 ZSVDET.

[15] Srov čl. 25 odst. 2 eIDAS.

[16] Srov. čl. 25 odst. 1 Nařízení eIDAS.

© EPRAVO.CZ - Sbíрка zákonů, judikatura, právo | www.epravo.cz

Další články:

- [Posouzení shody dle AI Act - zkušenosti z praxe](#)
- [Začínají soudy zohledňovat náklady podnikatelů při plnění právních povinností v oblasti e-commerce?](#)
- [Byznys a paragrafy, díl 35: Ručení za dluhy z podnikání u OSVČ a s.r.o.](#)
- [Bezpilotní systémy vlastní konstrukce v kategorii Specific: regulatorní požadavky a praktické aspekty](#)
- [Nefungující rozsah péče o dítě. Cesta přes využití terapie a dalších opatření podle ustanovení § 503 zákona o zvláštních řízeních soudních](#)
- [De iure traktor, de facto nákladní vozidlo, už ne tolik výhodná dualita](#)
- [Digitální důkazy z webu v soudním řízení: jak doložit, co bylo online zveřejněno?](#)
- [Pokuta 32 mil. EUR pro Dacia/Renault - evropské soutěžní úřady tvrdě došlapují na no-poaching. Měla by Vaše společnost být na pozoru?](#)
- [Rozdělení společného jmění manželů v případech výdělečné činnosti pouze jednoho z manželů](#)
- [Oběť znásilnění má nárok na peněžitou satisfakci](#)
- [Digitalizace AML povinností: jak technologie mění plnění povinností pro tisíce povinných osob](#)